TEACHERS' GUIDE

CYBERSECURITY & INTERNET SAFETY:

Starting the Conversation with Middle and High School Students

BARR ADVISORY

TEACHERS' GUIDE

CYBERSECURITY & INTERNET SAFETY:

Starting the Conversation with Middle and High School Students

How to Use this Resource

BARR Advisory has teamed up with a cohort of partners and clients to produce a video series designed to help educators and parents start and continue thoughtful conversations with their middle and high school students about cybersecurity and internet safety.

In addition to this teachers' guide, the package includes five videos featuring conversational, age-appropriate interviews with leaders in the fields of cybersecurity, technology, and software development on topics such as cyber careers and digital citizenship.

The videos can be shown separately or consecutively and are designed for students in grades six through twelve.

> *For students in this age group who are just beginning to establish their independence online, understanding why and how to take control of their digital footprint is crucial.*
>
> *—Devin Olsen, BARR Advisory*

Table of Contents

Suggested Activities and Lesson Plans

- **Watch Episode #1: Cyber Careers.** Afterward, provide students with a career interest and aptitude quiz. Once they complete the quiz, instruct students to write a journal entry reflecting on their results and whether they might enjoy a career in science, technology, engineering, or mathematics (STEM).
- **Watch Episode #4: Cyber Hygiene and discuss with students the proper protocols for reporting suspect phishing attempts.** Later, send a mock phishing email to students using an unrecognized email address. In the next class, reward students who report the email with a small prize and discuss what warning signs they found in the email.
- **Designate one week during National Cybersecurity Awareness Month in October to be your classroom's "Cybersecurity Week."** Watch one episode of the video series each day and discuss as a class.

EPISODE DESCRIPTIONS

Episodes can be shown individually or as a series and are available to view or download for free at BARRAdvisory.com.

1 **Cyber Careers**
Cybersecurity and technology professionals share their career stories and explore the many career options available to students who are interested in working in STEM fields.

2 **Internet & Social Media Safety**
Cybersecurity experts share tips for teenagers on how to stay safe online, including why some personal information should always stay private and how to safely use public WiFi.

3 **Digital Citizenship**
Cybersecurity and technology experts discuss how to be good citizens online, the dangers of cyberbullying, as well as how to recognize and report scams and phishing attempts.

4 **Cyber Hygiene**
Cybersecurity and technology experts discuss best practices surrounding cyber hygiene and personal identity management.

5 **Future of Cybersecurity**
Technology experts give their takes on the state and future of cybersecurity and tech, including artificial intelligence (AI).

MEET THE INTERVIEWEES

The video series features exclusive interviews with 12 cybersecurity, technology, and HR experts, including:

KERI BARNETT-HOWELL

Keri Barnett-Howell is the director of talent development at Mission Cloud, a trusted managed cloud services provider and AWS Premier Tier Services Partner.

DANIEL COLGROVE

Daniel Colgrove is the vice president of customer service at Broadleaf Commerce, a leading commerce software solutions provider supporting enterprise retail brands.

COREY EMERSON

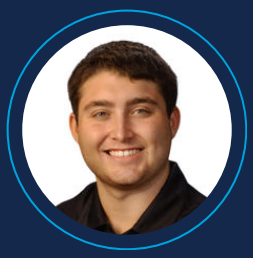
Corey Emerson is a security engineer 2 at Quickbase, a no-code platform for building custom apps, uncovering insights, and protecting data from risk.

BALAJI GOPALAN

Balaji Gopalan is the co-founder and CEO of MedStack, an award-winning and industry-recognized compliance solution for digital health.

JONNAE HILL

Jonnae Hill is the head of People & Culture at BARR Advisory, a cloud-based security and compliance solutions firm.



LARRY KINKAID

Larry Kinkaid is a cybersecurity consulting manager at BARR Advisory with over 10 years of experience in the cybersecurity industry.

JULIE MUNGAI

Julie Mungai is a manager on the attest services team at BARR Advisory. Prior to BARR, Julie worked in risk assurance at PwC.

ALEX NETTE

Alex Nette is the CEO and co-founder of the cybersecurity solutions firm Hive Systems and the co-founder of Audora, an award-winning compliance automation platform.

DEVIN OLSEN

Devin Olsen is a former educator now serving as an associate consultant on the attest services team at BARR Advisory.

STEVE RYAN

Steve Ryan is a manager on the attest services team at BARR Advisory specializing in healthcare compliance.

JESSICA WALTERS

Jessica Walters is the senior security and IT program manager at Tessian and the former chief of staff to the CISO of Cisco's Security Business Group.

TEMISHA YOUNG

Temisha Young is the senior auditor alliance manager at Drata, a leading security and compliance automation platform.

ABOUT BARR ADVISORY

BARR Advisory is a cloud-based security and compliance solutions provider specializing in cybersecurity consulting and compliance for companies with high-value information in cloud environments like AWS, Microsoft Azure, and Google Cloud Platform.

A trusted advisor to some of the fastest growing cloud-based organizations around the globe, BARR simplifies compliance across multiple regulatory and customer requirements in highly regulated industries including technology, financial services, healthcare, and government.

TALKING POINTS

Episode 1: Cyber Careers

TECHNOLOGY IS CONSTANTLY CHANGING AND EVOLVING

"If you like to do the same thing every day, all the time, technology is probably not the career path for you. But if you like to do exciting things, you like to do something different every day, that's the type of career technology can bring towards you if you're interested in it."

—Temisha Young, Drata

LEARNING IS A LIFELONG ACTIVITY

"Cybersecurity is an extremely fast-moving industry. People are constantly developing new technologies and new ways to do things, and it's important for those who work in cybersecurity to have a lot of curiosity and a drive to learn. Learning doesn't stop after graduation."

—Jonnae Hill, BARR Advisory

CONTINUE THE CONVERSATION:

- **Why might good communication skills be important for someone working in cybersecurity or technology?**
- **What other "soft skills" would you need to develop if you wanted to pursue a career in tech?**
- **What skills do you already have that will benefit you in your career?**
- **What would be a good first step for a student who wants to pursue a STEM career after high school?**
- **What local organizations or school clubs could you join if you wanted to learn more about technology?**

TRANSCRIPT

Episode 1: Cyber Careers

WHAT IS YOUR CURRENT ROLE?

KERI BARNETT-HOWELL: I am the director of talent development at a startup company that works alongside Amazon Web Services, so my day-to-day looks like constantly reviewing what our team is working on to make sure that they are developing in their own careers. We know now that people have to learn constantly in their careers; they constantly need to be developing. So companies have spun up departments like mine that are responsible for keeping everyone learning. I'm reviewing the tech landscape, I'm seeing what's coming out next, I'm seeing what training is available and developing new training for my team so that we can stay on the cutting edge.

TEMISHA YOUNG: My current role, I serve as the senior audit alliance manager at Drata, and simply that means I connect our thousands of customers to auditors who perform cybersecurity audits, so making sure that these companies have the right security things in place so they don't get breached by hackers.

JESSICA WALTERS: I am currently a senior security & IT programs manager with Tessian, which is a security product company that delivers a product that helps businesses secure their email platform and make sure that emails aren't incorrectly sent out.

JONNAE HILL: [As head of People & Culture at BARR Advisory], I have the amazing opportunity to help shape what our company culture looks like, to keep an eye constantly on if we are providing the support and the tools needed for all of our team members to succeed. It's an amazing job.

WHAT DOES YOUR DAY-TO-DAY TYPICALLY LOOK LIKE?

TEMISHA YOUNG: The day-to-day is pretty fun. I interact with lots of groups in my company. Some of those groups are our product team that actually design and implement the product, engineers who do the actual design and the engineering of how the products actually work, and then also I get to interact with auditors, and those auditors are people who come in, like I mentioned before, and actually assess a company to make sure that their security posture is efficient for whatever type of company that they are and the type of data that they have. It's a very fun role because I don't do the same thing every day and I'm always interacting with people across different roles in my company.

JONNAE HILL: Most of my day-to-day involves interacting with our team members, so that might be talking about what learning and development opportunities they need or ideas that they have to bring our company together and learn about each other. It's a really great opportunity for me to spend most of my days—I'm head of People & Culture, so it's interacting with our people, because they have the best idea of what could be possible for our company.

JESSICA WALTERS: Being a program manager or a project manager, these are roles that can look very different depending on the team size, the organization size, and the needs of the business. My day-to-day really looks different depending on what my team and my CISO need in that moment, so it could be anything from working on a strategy for a really long-tail project that our security organization would like to deliver to Tessian, or it could be as simple as working through our queue of vendor security questionnaires that we're responsible for reviewing and providing our approval on as the business considers new vendors that we want to engage with.

WHAT KINDS OF TASKS WOULD YOU SAY YOU SPEND THE MOST TIME ON?

TEMISHA YOUNG: That's a great question. I think mostly interacting with auditors. I interact with them and we talk about some of the things that they're doing with our customers, and so I'm getting feedback from those auditors and making sure that our product meets those needs. So my background in cybersecurity is very important with understanding what the auditors are seeking and looking for so we can better prepare our customers for their cybersecurity audits.

KERI BARNETT-HOWELL: I spend a lot of time doing research and I spend a lot of time on data analysis. I look at a lot of what our team is doing day-to-day and seeing: Is it effective? Are the training programs that I've created, are they working? Are people learning? Are they growing? And I also spend a lot of time reaching out to community partners to work with schools and to work with other organizations to tell people about careers in the cloud. Not many people know about them right now. This may change as you get older, but right now there's no college programs and there's no really good training programs to create cloud and DevOps engineers. So I spend a lot of time thinking about how do we create those and helping people get into these types of careers.

JESSICA WALTERS: I spend the most time communicating, whether that's in written form or verbally, so I think strong communication skills are something that is important. I also spend time problem-solving, so thinking about problems that my team faces and figuring out how I can help enable us to overcome those.

JONNAE HILL: Right now, we are looking at all of the things that we want to accomplish in the next year. So in my day-to-day right now, the big projects that we're working on are what we need to do to get to our goals. Do we need some new tools to help our teams work more productively? Do we need to get together more so we can better understand each other and be better teammates to each other? So it's looking at some big-picture ideas for what we need to do to help our company get where we want to go.

WHY DID YOU DECIDE TO PURSUE A CAREER IN TECHNOLOGY?

TEMISHA YOUNG: As a child, I always had a computer, and so I was always learning, playing games on the computer, and I always knew I wanted to do something in technology. I went to college, I have a degree in chemistry with a focus in computer science, so I started my career out actually not in technology, but it was something that I always did on my own, so always up to date on the latest technology trends, learning new softwares—it was just a hobby of mine. And so I had the opportunity to change careers and that's how I switched into cybersecurity and technology.

JONNAE HILL: Prior to coming to BARR, I was working with students who wanted to get into the tech industry, and it was so interesting to me. I was around the learning and the teaching of what needs to go on to be successful in a career in tech. And so when this opportunity came to be, I wanted to jump on it, to be able to take those skills that I knew and actually apply them in the tech world.

The tech industry is so fascinating because it's changing all the time, so it really allows you to stay in a constant point of learning for yourself. There's always something new to learn. Every single day, something comes across my desk that I don't know about and I need to learn. And the great thing is when you surround yourself with really smart, talented people, there's always someone that can help you, and that's what's great about BARR, too. The tech industry, there's something for everyone, and it's a great environment to learn and always stay on top of new things coming your way.

KERI BARNETT-HOWELL: As you might find out as you get older, careers are not straight-forward. I started out in healthcare and I didn't really like it that much, and so I moved into a startup company that was pursuing new AI technology for healthcare. And I just fell in love with tech. It was so dynamic. Every single day, something changes and something new comes out.

So when I transitioned to my current company, which does cloud careers and cloud consulting, I had to learn this whole new vocabulary about tech, about the infrastructure behind the scenes, and it was so cool—I had never heard of how these things work. For example, when you are playing a video game at home and you are making moves and doing something and you're playing with someone who's totally across the world, say in Morocco, and both of you are seeing the things happen instantaneously. That didn't just happen. We had to build that infrastructure so those things can happen at the exact same time in a totally different part of the world. And so the internet, as you know it, it's not something that is just static. We are constantly building it, constantly developing it, and finding new ways to have people be connected. I really just fell in love with it, but it was an accident that I got here, and it's been a super exciting time to learn more.

JESSICA WALTERS: My path into technology was actually not one that I had planned on. I graduated college with a communications degree and really didn't have a strong feeling about where I wanted to land, so I took a chance at a local company. I spent about five years there just learning about all parts of the business; I was an executive assistant. And then eventually, that career choice led me to a tech company called Duo that develops a multi-factor authentication product, and my path in Duo was really just trying new things, so having the opportunity through the relationships that I built to take on roles in IT and eventually security. And it's been the most fun unplanned adventure of my life.

DID YOU GO TO COLLEGE OR PARTICIPATE IN ANY INTERNSHIPS?

JONNAE HILL: I attended college at the University of Missouri and I studied communication and psychology. Something that has always interested me is just how humans interact and the collaboration among people, and the thing with the communication aspect is we need it in any type of job that we're doing. Every single person needs strong communication skills, both in the work they do and in just how they interact in the world. And then I had the great opportunity to seek out internships throughout my time in college. I tried to do one every single summer with different types of organizations so I could learn about different businesses, but also different lines of work, to figure out what I wanted to do, what kind of business I wanted to be in. And it was great because those internships gave me the chance to find out some of what my passions were and follow them, but also I learned a lot of the things that I didn't want to do. So it's equal parts ruling stuff out and really getting to embrace what you really love to do.

KERI BARNETT-HOWELL: I did go to college. I got a degree in history, which does not translate into any careers. And after that, I went into the Peace Corps, where I spent two years in China teaching English. And then I got a master's of public health. And so I really could not have predicted how all of those things would have come together, where I learned how to be a teacher. I learned how people learn. As I was working, I realized that I was just very good at teaching people things. I was very good at understanding how to break things down and teach it to others. And at that same time, there was a big need for companies to be able to train people and continue their growth within, and so those things happened together. I fell into this, but everything that I've done in my career and everything that I've learned has contributed to being able to do my role effectively. When I got my master's in public health, a lot of what I

learned was how to look at data and how to do data analysis. That's a lot of what I do now. Nothing you learn is going to be wasted; it's all going to go towards your future career. You just may not see how everything comes together now.

TEMISHA YOUNG: I actually did what is called a cybersecurity boot camp. So it's like, maybe a half-year course that you really go in and you do a deep dive in a specific area of technology, and that was cybersecurity for me. I took that course at Emory University, and so that really gave me a strong foundation in cybersecurity.

From there, I studied for a certification, which is really big within the tech field. There are all types of certifications that you can take. The one that I prepared for and studied for was called the CompTIA Security+, and that is really a foundational cybersecurity, agnostic type of certification. Once I got that certification, I used that to do some volunteer work for some nonprofit organizations, so it wasn't a traditional intern, but it was a local organization that I was passionate about and they needed some help with understanding security. And so that gave me some real hands-on experience before I started my career in cybersecurity.

JESSICA WALTERS: I did participate in two internships during my college time, and neither were related to what I do today, but both were really interesting opportunities for me to just get my feet wet in a working setting. And I think those experiences really helped me understand that it's just as important to figure out what you don't want to do as it is figuring out what you do love to do.

HOW DID YOUR PAST JOBS PREPARE YOU FOR YOUR CURRENT ROLE?

JONNAE HILL: Some of the early roles that I held, again, going back to that people-driven kind of nature, I was a recruiter for a company. So I got to help decide what candidates that might be a fit for our company, help guide them through our interviewing process, and then onboard them and see them through their early stages of that job in our company, so that was an excellent opportunity. Then also, as I mentioned, I worked at a university helping and advising students on their educational journey. It happened to be students in the technology, STEM, and business fields. I worked alongside them to help them reach their educational goals, but also get out there and find some of those internships that I had such a value in. I wanted to share that with others and get them keyed into those spots that might help them as well.

TEMISHA YOUNG: My first role in cyber-security, I was an IT security analyst for the Georgia Department of Public Health, and it was one of my favorite careers. It allowed me to understand how broad cybersecurity was. I did roles from access control, to incident response management, internal auditing—so that's how I got the auditing bug and found out that I actually liked auditing. I also did our cybersecurity awareness training program for all of the Georgia Department of Public Health, so it allowed me to learn what I liked about security. Cybersecurity is very broad, and so helping and understanding what you like and what domains of cybersecurity that you're interested in helps you to understand the track you want to go in your career.

WHAT SKILLS ARE USEFUL FOR JOBS IN TECH AND CYBERSECURITY?

JONNAE HILL: Cybersecurity is an extremely fast-moving industry. People are constantly developing new technologies and new ways to do things, and it's important for those who work in cybersecurity to have a lot of curiosity and a drive to learn. Learning doesn't stop after graduation.

TEMISHA YOUNG: Skills are important, and not just tech type skills, but really intuitive skills. So like a problem-solver, right? There's so many problems to solve in technology and

cybersecurity, so you've got to be inquisitive. You've got to be the type of person that likes to ask questions, to learn constantly, because technology and cybersecurity is forever changing every day. There are always new things, new programs, new applications, new risk that you have to be aware of. So if you're a problem-solver and inquisitive and love to learn, I think that's a great skill to have.

Another one is not afraid of change. If you like to do the same thing every day, all the time, technology is probably not the career path for you. But if you like to do exciting things, you like to do something different every day, that's the type of career technology can bring towards you if you're interested in it.

And I think the most important thing is integrity. You're making big decisions about companies in my role as an auditor. I have to make sure that these companies are doing the right things, as a former auditor, and just making sure that they are meeting the requirements to meet certifications. And then just integrity in how you carry yourself in your role, being able to alert your company leadership if there's something you see that may not be okay—those are the types of qualities outside of just those technology skills that you'll learn along your way as you're either in school or self-taught.

KERI BARNETT-HOWELL: My entire career is dedicated to keeping my engineers learning. Every single year, new technologies come out, new things happen, and so you need to be the type of person who loves to dig into things, pull them apart, figure out how they work, and put them back together again. Curiosity is the number one skill that we look for.

Good communication skills are extremely important for cybersecurity professionals, especially those of us who work from home, like myself, which is a lot more common nowadays. Not everyone has to be a public speaker, but it's a great skill to work on, and you only get more comfortable with practice. I also use email and messaging tools like Slack almost every day at work, so being able to express my thoughts in writing is crucial.

And I have to say, for those of you who are thinking about engineering careers, it's very, very important to be able to communicate. You need to be able to communicate something technical to somebody who may not understand that. Learning how to translate things and talk to people, such an important skill. And especially in cybersecurity, there's lots of these types of projects where everyone is working on one small piece, and your piece has to fit in with the rest. So, communicating with your team and understanding what they need, that's crucial to being a good part of any company.

JONNAE HILL: From the lens I look at it, the two big ones would be the ability to communicate with each other in multiple formats—so we're talking communication like we're doing now, like over a screen, also in-person settings. And typing, right? So much of the communication that we do with each other, especially now in the days of remote and hybrid work, we might not be sitting at a desk right next to someone that we're working on a project with. So it's important for us to be able to clearly communicate back and forth via writing, email, text messages, whatever that looks like. And in the spoken word, too—getting your point across, being empathetic in how you are communicating with people so that everyone's comfortable and feels that they are in a trusting space that they can share their ideas to come up with the best solution to solve the problems in your business.

In order to do any job, whether it's in the tech field or beyond, you have to be a good team-mate. And so that means doing what you say you're going to do, fulfilling your requirements for your job, and being respectful among your team so that you can collaborate together and have the best outcomes for what you're working on.

JESSICA WALTERS: Since COVID, so many of the jobs in tech have been moved to work from home, and so that makes this skill that much more important. It doesn't mean that you have to necessarily be the best public speaker or perfect in everything that you deliver, but I think that you have to have a comfortability with working on those things, because you'll get better with practice.

I would say that figuring out how to communicate effectively asynchronously is really important too, and what I mean by that is you may not always be having a live conversation with others. You may need to convey your thoughts via chat tools like Slack or emailing, and that's really important too. You're going to want to come into new roles with an open mind, where you're curious, willing to learn, excited to share ideas, and express your opinions in a way that helps move the entire team forward.

TEMISHA YOUNG: Good teamwork is also essential in any workplace. You have to be able to collaborate, share ideas, and express your opinions, even when you disagree sometimes—and that definitely will happen. Sometimes in my role, we work on big projects, and sometimes small tasks that need to be done along the way. You can divide and conquer, so that's why teamwork is so important. You have to be able to depend on one another and trust that everyone will complete their assignments. And when we all work together, we can all accomplish some pretty big goals.

WHAT OTHER TECH CAREERS ARE OUT THERE THAT STUDENTS MIGHT NOT KNOW ABOUT?

JONNAE HILL: That's the other just amazing thing about the world of technology and careers in technology—there's truly something for everybody, and almost on a daily basis, new opportunities are coming out. So whether your interest is to be a coder or to do audits or to find ways to reduce cybersecurity risk—if that's your interest, that's fantastic, because there's so many opportunities for you. But something I also encourage you to think about, even if maybe that isn't where your passion lies—take me, for example, my career has taken me a couple of different places, but there's still a space for me in the technology world, helping businesses create the most wonderful, thriving environment that they can for the people that are doing their specific tech-related jobs. So even if you're interested in the field of human resources or community engagement or marketing or business development and sales, all tech companies need people like you. I definitely encourage you to just think about that. There's a spot for everybody in a tech career.

TEMISHA YOUNG: When I started my cybersecurity journey, I was thinking maybe I would be a pen tester or someone who was doing something a little more technical, more hands-on technical. But once I got into my career, I saw the skill sets of me being very efficient, very thorough. And auditing, I really enjoyed that internal auditing piece. And just to explain what that is, so there would be teams within our organization and I would go through and make sure that those teams were meeting the requirements that were specified by HIPAA, in particular, because I worked for the Department of Public Health. I was very thorough, I took really good notes and could give good feedback and communicate well. Auditing may not be something that you may think about, but it may be a skill set that you may have, and so think about auditing as a career.

KERI BARNETT-HOWELL: A huge one is consulting. A cybersecurity consultant helps companies figure out what they need to do to minimize the risk of a cyberattack. A consultant might give advice to the company's leaders and help with internal audits. This is a much more complex role than it might sound like at first. When talking about cloud cybersecurity especially, there's so many different ways for

companies to protect their environments, and so the cybersecurity consultant needs to understand all of those ways, what is good, what is bad about each of those, and how to recommend them to a company. There's always trade-offs when it comes to security. If you have a fully secure environment, that means absolutely no one can get into it, and that's not very useful. So you need to figure out ways to maximize the ease of the environment and also maximize the security. It's a very complicated role, and good consultants are hugely in demand.

TEMISHA YOUNG: And another one if you're creative, marketing. I'm a creative soul deep down inside, and so I like to market. I like to express myself in different ways. And so if you're technical and you have that creative mind, I think marketing is one of those things that you may not think about, but these cybersecurity companies—and there are thousands out there—need someone to market their products, inform their customers about some of the services that they offer. There's so many different avenues, so if you're not as technical and you still love technology, there's so many things you can do. Everyone, just about, could be in technology. You just have to find the right role that works for you.

JESSICA WALTERS: Another non-technical role that really helps enable technical teams is a program or a project manager, like what I do. These are really what I refer to as "glue roles." They're roles within the team, people within the team, that help ensure that the team is able to develop a strategy and deliver on that strategy. You don't often have to have full understanding of what your team is working on, but you're there as someone that can enable them to deliver their best work.

Lastly, I would say that product managers within security product companies is a really interesting space to explore. These are people that work to understand what customers need from a company. When you're building a security product, it's really important to understand the voice of your customers and product managers, and that context can really make a difference.

KERI BARNETT-HOWELL: Another role: Cloud analysts often need to know a lot about security to be able to recommend different types of solutions to their customers. So a consultant is someone who, often, they understand the deep engineering and can build different secure environments; the analysts can actually go in and look at an environment and say, how secure is this? And what else needs to be done to make this environment more secure?

JONNAE HILL: Many companies want or have to prove that they're keeping their employees' and customers' data secure. For instance, hospitals and doctors' offices must make sure patients' personal health information is kept private. And one way for a company to prove they're keeping up with cybersecurity laws and regulations is by asking an outside auditor to give their opinion, and that's something we do here at BARR. A security auditor's job is to look closely at the company's cybersecurity processes and decide whether they're working correctly.

TEMISHA YOUNG: Pen testing, which is also known as ethical hacking—people with this job are paid to actually hack into company networks, and really their goal is to identify weaknesses so that companies can fix and become better when it comes to their security environment. I know a lot of times you hear about hackers as "the bad guys," but you can actually do hacking and help companies. Because if nobody actually penetrates or tries to penetrate their environment, they may not know they have weaknesses—maybe with access control, or maybe they haven't updated a software in the allotted time that they should. This is a really fun way of being in a cybersecurity career, and so if you're into hacking, there's some great ways to do it ethically, and that's called pen testing.

KERI BARNETT-HOWELL: Technical writing and editing is another big role. In cybersecurity, technical writers and editors might work on

things like auditor's reports and company policy documents. These jobs combine multiple skill sets. Technical writers don't just have to be great at writing, but they also have to be comfortable with topics related to cybersecurity and technology. Technical writing is another role that's often overlooked, but it is hugely in demand. It's very difficult to do well—to write something super technical in a way that everyone can understand it. So this is a great job if you enjoy writing and you enjoy explaining things to people, this could be a great role for you.

JESSICA WALTERS: I would say that the biggest takeaway to remember is that not all roles within cybersecurity are technical. You don't have to have a full understanding of coding or the behind-the-scenes on how to build something to really be able to make a difference and join a security team.

WHAT ADVICE WOULD YOU GIVE TO STUDENTS WHO ARE INTERESTED IN PURSUING CAREERS IN TECH?

JONNAE HILL: I'd encourage you to find ways to discover what's available, and that could be checking out new clubs or organizations or extracurricular activities at your school. Talk to your teachers, especially the ones that are teaching in the tech space. They're a great resource and know opportunities in the community. That might be a "capture the flag" event or a robotics team, but I encourage you to explore, check stuff out, even if you're unsure at first. It's wonderful to put yourself in a position to try something new—and it might be something you love and it might not, but it's still a learning experience and worth the try.

TEMISHA YOUNG: For me, I think one of the most important things you can do is attend conferences. There's so many conferences, virtual conferences, those you can go to in-person, that allow you to really learn about an industry in technology, in cybersecurity, meet some amazing people, learn about the new trends that are coming along. And when you build that network, that's how you build relationships to get internships and job opportunities. You'll meet companies that you've never ever heard of at these conferences, and you may find that company is the perfect company for you. So anytime you can attend a conference or meeting related to technology or cybersecurity, I think for me, it has been most beneficial with attending conferences.

Also, as a student, you have the ability a lot of times to attend these conferences for free or at a very discounted rate. So make sure when you visit their website, they usually have a student section where it has more information so you can register as a student. There are also different tracks at those conferences as well geared towards students or people who are looking to pursue a career in technology or cybersecurity, so definitely take advantage of the offerings as a student, even with certifications as well.

JESSICA WALTERS: My best advice would be to get involved. It could be on networks like LinkedIn or other tech communities online. There are a lot of online resources that I think are easily accessible and can help you learn a lot about areas that you might be interested in. So, for example, you could Google, maybe, a type of coding that you're curious about, or you could Google a topic like two-factor authentication, which is something that's really important in the tech industry and keeping companies secure. And these are all concepts that there's a wealth of knowledge online that you can tap into. There's also a lot of well-known blog writers online that write about topics that are really relevant to what's going on today and are a great source of free learning that you can tap into.

Lastly, I'd say go look at companies that are building products that you're curious about, whether that's Duo Security and their two-factor authentication or Tessian and our email security

products. Most of the companies that are building these things have a lot of information right on their website that can help you understand why it's important and how to use their product, and these are all things that will help feed your curiosity and lead you to more information that is really interesting to you.

KERI BARNETT-HOWELL: If you're thinking about college, think about majoring in a STEM field: science, technology, engineering, or math. These degrees prepare you for careers in many different industries, including cybersecurity. But you don't need to have a computer science degree to work in tech. If you want to be a technical writer, for instance, you might choose to study writing or literature.

I would also recommend working on things at home by yourself. Try to do projects on your own. Spin up new websites. Learn how to use the tools on your own. Work with your family. Have some fun times building things, breaking things, getting your hands dirty. It's really useful when it comes to future careers in engineering.

JESSICA WALTERS: Be bold and try something new and don't be afraid to fail. Failing is part of the process and you really can grow so much in something that you try and don't get right the first time.

KERI BARNETT-HOWELL: I think that any career that you go into in tech, you're going to need to know something about security. So all of these security things that you hear about, keep them in mind, because it's going to help you in your future career. There's no career in tech that doesn't touch on security in some way, so try to learn as much about it as you can. It's only going to benefit you.

TALKING POINTS

Episode 2: Internet & Social Media Safety

MINIMIZE THE DATA YOU SHARE

"If you're signing up for a social media account, it does not need your Social Security number. There is no reason for that. But if you're working with your doctor and signing up for an online portal, they may need some additional information to be able to validate who you are, like through your insurance information or how to bill you. Think about who you're sharing with, and think about the minimum amount of information that you want to share."

—Alex Nette, Hive Systems

THINK BEFORE POSTING PUBLICLY

"If you take pictures in the world, it's very easy for somebody who might have not-great intentions to find where you are just from the picture that you took, even if it seems innocuous. You can be exposing unintentionally where you live or where you hang out, and not everybody that can see your information on the internet is your friend. In fact, most of them aren't."

—Corey Emerson, Quickbase

CONTINUE THE CONVERSATION:

- **Your friend can't decide whether to set their social media accounts to"public" or "private." What advice would you give them?**
- **Why do you think college recruiters might consider an applicant's social media profiles when making a decision?**
- **What are some of the risks associated with using public WiFi networks?**
- **How much screen time is too much? What are some ways you could reduce the amount of time you spend on your devices each day?**
- **Why is it important to review your privacy settings on every app you use?**

TRANSCRIPT

Episode 2: Internet & Social Media Safety

WHAT ARE THE BEST WAYS FOR STUDENTS TO STAY SAFE ONLINE?

STEVE RYAN: Keep your personal information private. Throughout this conversation, we'll share more detailed advice on how to do that, but a great place to start is on social media. It can be very tempting, especially with everything we see on TikTok, Instagram, X, what have you, to create that public profile to become that next huge influencer. But you should be really careful about what you're sharing publicly online.

JULIE MUNGAI: I recommend avoiding public WiFi networks. These are not secure, meaning it's easier for hackers to gain access to your private and personal information. Exercise caution before you share. You might have heard the saying, "the internet is forever," and this is true. Even private social media posts and text messages, all of these items can be screenshotted, and once you hit send, you can't take it back.

COREY EMERSON: Keeping your information as private as possible is the best way to keep yourself safe on the internet. Don't post about where you are. Make sure you have location turned off on any of your social media apps. If you take pictures in the world, it's very easy for somebody who might have not-great intentions to find where you are just from the picture that you took, even if it seems innocuous. You can be exposing unintentionally where you live or where you hang out, and not everybody that can see your information on the internet is your friend. In fact, most of them aren't.

There are people that do this on streaming services, or streaming like TikTok. People will get a picture, or they'll get a pin dropped in somewhere in Google Maps, and just from context clues, they have no idea where they are, they have to figure out where they are. And people do it, and it's terrifying.

JONNAE HILL: Just something to think about as you're communicating or posting: A good rule of thumb is to avoid posting anything negative about other people. Your school, another person, a sports team—any of those things—you might be given specific instructions from them about what not to post. But just even on a personal note, not putting anything out in the world that you wouldn't want them to see, because it will be there forever.

WHAT PERSONAL INFORMATION SHOULD BE KEPT PRIVATE?

ALEX NETTE: The best idea here is to always limit your information online that you share to the information that needs to be shared. So, if you're signing up for a social media account, it does not need your Social Security number. There is no reason for that. But if you're working with your doctor and signing up for an online portal, they may need some additional information to be able to validate who you are, like through your insurance information or how to bill you. Think about who you're sharing with, and think about the minimum amount of information that you want to share. Maybe instead of sharing your entire address, you just share your city instead. Always think about those opportunities. The hard part is once you've shared your information, it's hard to unshare it. Even if you change it later on, oftentimes it is still logged in and tracked, so make sure that the very first time that you think about sharing, you stop and consider what you want to share.

JULIE MUNGAI: Information that should be kept private is information that you don't want to share publicly. So two things to think about on whether or not you want to keep something private or public: Think about your safety and think about your future. Most important is, of course, your safety. You never know who's out there and who you're really talking to online. You also want to think about your future. Before you post anything online, ask yourself whether it's something that you would want recruiters for college or future employers to see. Even private posts can be screenshotted, so if you're not sure about whether posting something is appropriate, talk to a parent or a teacher or any other trusted adult and really understand what the implications are.

JONNAE HILL: And even if you're doubting it, that's probably a sign you shouldn't post it. Some information you never want to share publicly, that would be your location, where you live, your school name, your home address, and of course, your passwords. It's also a good idea to think twice about posting photos. You want to avoid sharing photos of documents that you have personal information on, and report cards, your driver's license, things like that, that hold a lot of personal information. You do not want that posted publicly.

COREY EMERSON: You don't want your phone number out on the internet. If you go by a handle, you don't necessarily always want that handle to be able to relate to your full name. You don't want where you live to be on the internet. You don't want the town you're in to be out in public. The more details that you can hide away and keep hidden, the better off you are.

STEVE RYAN: A great way to check out what information is publicly available about you online is to switch your browser to incognito mode and Google yourself. This is going to allow you to see what your future employers may see or what your college recruiters are going to see. If you find that public Instagram profile that you don't want anybody to see online, you can switch that to private.

JONNAE HILL: In the spirit of what you're putting online and really thinking about what you post or what you share about yourself online and the longevity of that—that it never goes away—think about that before you post something. Is this something you would want a potential employer to see? So, you want to get a job down the road. Just think, would you want that person that's interviewing you to look back on all the posts that you've shared on social media and see some of the things you've posted? Because they're able to. So it's easy to quickly post something in the moment, but it really is a good rule of thumb and something to think about before you put anything out there: Who might be seeing this in the months, years to come? Because it'll always be there.

JULIE MUNGAI: I'm sure the person that you are online today is going to be different than the person you want to portray when you start looking to get into college, when you start looking for jobs, and later on down the line, so always be cautious and get advice from any sort of trusted adults around you.

HOW SHOULD STUDENTS ADJUST THEIR PRIVACY SETTINGS ON SOCIAL MEDIA?

ALEX NETTE: I love this question. If you've never been into the settings menu in any of your social media accounts, you're doing yourself a huge disservice. Go there now, whether it's TikTok or Instagram or any other new app that's coming out next week. Make sure you dive into that settings menu immediately. Oftentimes, you can limit tracking and ad preferences.

Some things, unfortunately, you can't limit, and as a result, that's often part of the terms of service of using that app. So be careful what you are putting in there. But if there's an opportunity to reduce the way that your information is being

used or shared, whether it's creating your account as private versus public, or when information gets shared out publicly, even if you had to input it into the website—for example, putting your birthday in, but not sharing it—those fields in there in that privacy menu in the settings menu are going to be the best way to control how your information is shared.

JULIE MUNGAI: The best way to keep your social media profiles locked down is to set everything to private, so only people that you've added as your friend or you've approved as a follower can see what you post. Working in the cybersecurity field, we know that there will always be some risk involved in using social media.

JONNAE HILL: The only way to be 100 percent certain that your personal information stays private is to never post online, and we know that's just not realistic. But what you can do is minimize your risk. If you and the trusted adults in your life decide that you do want to post publicly on social media, consider only sharing your first name and not your last name, or be more selective about it.

STEVE RYAN: For instance, on platforms like TikTok, you can change your privacy settings for each individual video that you post, so not everything has to be public all the time, and you still might be able to be that big influencer one day.

WHAT ABOUT OTHER SITES, APPS, AND SERVICES?

JULIE MUNGAI: This does not just apply to social media. Use the same rules to stay safe on messaging apps like iMessage, WhatsApp, Snapchat, and more, and across all of the devices that you use, from your cell phones to your smartwatches to your school laptops and even video games that allow you to play online with others. If you must talk to people who you don't actually know in real life, avoid sharing any personal information that could be used to identify you, like your school or the city that you live in.

ALEX NETTE: We spent a lot of time today talking about social media, but there are so many other ways that we use the internet for managing our day-to-day lives. Think about bank accounts, emails, your school, eventually how you'll work at college and your workplace afterwards. All of those start to form our online identity, so everything that we've talked about that relates to social media also applies to all of those sites. If you get some new gadget to hook up to your house and play with, and it asks for an online username and password, use those same tips and techniques that we talked about—long, unique passwords, and multi-factor authentication if it's available—every time. Whether social media, bank accounts, or otherwise, those are all important to you. Make sure you don't lose access or have your information stolen because of bad security choices.

WHAT SHOULD STUDENTS KNOW BEFORE USING PUBLIC WIFI?

STEVE RYAN: Be careful about connecting to public WiFi. When you're at Starbucks or a hotel or an airport, you might see signs saying they have free WiFi, but you should really think twice about that before connecting your devices. It's much easier for cybercriminals to access your information when you're using public WiFi because those networks aren't set up with the same protections you have at home or at school.

JULIE MUNGAI: Someone with bad intentions might even set up a fake WiFi network that looks real. If you have to use a public, unsecured network, check with the establishment to make sure that you're connecting to the correct one. Do not access sensitive information like your bank accounts or any password managers using public WiFi networks.

ALEX NETTE: If possible, use your own hotspot or VPN instead. VPN stands for virtual private network, and it's a service that your family or school can pay for that offers an extra level of protection when you're browsing the internet on a public network. VPNs work by encrypting your data, meaning that it's protected from hackers and scammers looking at it. It scrambles everything that you're sending across the internet, but when it reaches its destination, it gets unscrambled so that you can access that specific site. The idea is that it protects it, because no one can breach that VPN connection. Generally, they're relatively cheap, a couple bucks a month, but it's a great option if you're going to be constantly accessing data away from your home or school often.

WHAT ARE SOME EASY FIRST STEPS FOR STUDENTS TO TAKE?

ALEX NETTE: I've got five steps that I generally recommend to reduce your risk.

The first is go into your settings on apps like TikTok, Instagram, or any other social media site and look through all of them. Make sure your profile is set to private if you can, or at least look through the privacy settings to see what information is being shared on your profile or with that social media company.

Number two, remove and delete any personal information that you don't want to be shared, like your school or your home address. Those aren't things that need to be provided on social media, but for other accounts, like banking sites or your doctor, you may have to share that information, and that's okay.

Check to see if you've been sharing location data. That information can be shared either through the posts that you're putting, or through the photos that you're posting as well, which add that as what's called "metadata." Remove that from past and future posts to make sure that no one knows where your location is or where those photos have been taken.

Number four, it's easy for someone to create a profile with your fake name and photo, so only add friends or accept followers who you actually know in real life. If you think it's a new profile from a friend that you know in real life, reach out to them and ask them. Say, "Hey, did you request to follow me on Instagram? Did you get a new account? What's going on?" And if they didn't, make sure you report that profile for impersonation.

Finally, strongly consider limiting your screen time. The longer you look at your phone or screen or you have it too close to you, plain and simple, it's going to hurt your eyes in the long term. The other thing, of course, it does is it creates that "doom scroll of death" where you constantly are just scrolling through social media and you don't stop. You're not getting any more benefit out of it, and you're definitely exhausting both your mental health and your eyes. Take breaks regularly. Step away and find something else to do out in the real world, and even just get outside for a few minutes, and then come back to what you were working on.

These five tips will help you immensely, especially as you move up through school, into college, and eventually the workforce.

TALKING POINTS

Episode 3: Digital Citizenship

THE INTERNET IS FOREVER

"When you're in a conversation live with someone, you can really seek to learn and be a lot more flexible in the way that message is delivered. But when you do it online, it's very hard to walk that back, and it's there forever. Anything you say online, regardless of your intentions, will be there."

—Jessica Walters, Tessian

THERE'S A REAL HUMAN BEHIND THE SCREEN

"We have to be careful about what we say online, because the consequences of making somebody feel bad online are the same ones that may actually be reflected in the real world. Words hurt at the end of the day, and words matter, so what we say is really important."

—Alex Nette, Hive Systems

CONTINUE THE CONVERSATION:

- **Social engineering attacks have grown more popular in recent years. Why do you think that is?**
- **Why is it so important to report suspected phishing attempts?**
- **Have you ever witnessed cyberbullying? How did you respond? What will you do differently next time?**
- **What advice would give to someone who has been the victim of cyberbullying?**
- **Have you ever posted something online that you weren't proud of? What steps can you take to avoid that situation in the future?**

TRANSCRIPT

Episode 3: Digital Citizenship

WHAT IS DIGITAL CITIZENSHIP?

ALEX NETTE: For me, digital citizenship is this idea that we, as all citizens of Earth, have a duty to each other both to live in a society and respect each other, and that percolates into the world of online as well. In the digital age, it's a little bit different, because rather than encountering somebody on the street or in person, you're likely just to see a username or a handle. The idea is that the same rules that we follow day-to-day in our in-person lives should apply to our digital lives as well.

STEVE RYAN: You may have heard about citizenship in the context of your community. Good citizens are responsible. They do their best to help others. They share their opinions respectfully. And they follow rules set up by society to keep everyone safe. Digital citizenship is essentially the same thing, but it's just the online version of that.

Being a good digital citizen means that you have the knowledge and skills to engage with others safely and responsibly online. That includes on social media, on school message boards, video game lobbies, and everywhere else you interact with people on the internet. Really, a good digital citizen is a role model for others on how to be respectful and to do the right thing. We've all heard the saying, "If you don't have anything nice to say, don't say anything at all." It's especially true online where unkind comments can quickly go viral.

WHAT ARE SOME GOOD RULES OF THUMB FOR BEING COURTEOUS AND RESPECTFUL ONLINE?

ALEX NETTE: A good rule of thumb here in the world of being a good citizen online is remembering that even though you may just see an avatar or username for someone online, there's a real person behind that account. So whether they've said something inflammatory or you're interested in saying something inflammatory back, remember that there's a real human with real thoughts, real emotions. There may also be a chance that you actually know that person in real life, which has consequences associated with it, whether it's a classmate, or a colleague, or even somebody else in your family.

JESSICA WALTERS: First and foremost, I would say if you're not willing to say something directly to someone's face, then it's probably a good rule of thumb to not say it online. Saying hurtful things, or even things where maybe you don't fully understand the context but you're expressing an opinion—when you're in a conversation live with someone, you can really seek to learn and be a lot more flexible in the way that message is delivered, but when you do it online, it's very hard to walk that back, and it's there forever. Anything you say online, regardless of your intentions, will be there. I would say the best, easiest rule of thumb is to take a pause, think about if you'd have that conversation in person, and if not, maybe hold off and save that thought for another, more appropriate time.

DEVIN OLSEN: Treating it as a face-to-face conversation, remembering that there is most likely another human being on the end of that screen, wherever you're talking or texting to. So I would treat every conversation that you have online, especially when you are relying on anonymity to protect you, as a face-to-face conversation. If you wouldn't say something to somebody's face, don't say it online.

STEVE RYAN: Honestly, this advice applies to everybody, whether you're a student, whether you're at the corporate level—when doing your day-to-day jobs, just slow down. Before you hit publish, take a beat and reflect on what you've written. Does it really represent who you are? And not only that, but if you were reading that without it being your own writing, how would you interpret that? How would that come across?

Long story short, don't post anything you wouldn't want your family, your teacher, or your future boss to see, because as we know, if it's on the internet, it does not go away. And along the same lines, remember to be kind when posting on social media, even and especially when posting anonymously. If you're feeling frustrated or overwhelmed, walk away from your device and come back later. Frankly, that's some advice I give to people on my team, especially in some frustrating circumstances we have here. It's really easy to get tunnel vision. But there's more to the world than just what's behind the screen. If your online interactions are starting to negatively affect your mood, try taking a walk, reading a book, take the pup out, play some basketball with your friends, what have you.

WHAT IS CYBERBULLYING?

ALEX NETTE: Cyberbullying, for me, is just the same as real bullying in the real world. It's ultimately making somebody feel like they are less than themselves, feel bad about themselves, or bad for some of the actions they may have taken, even if that's not justified. We have to be careful about what we say online, because the consequences of making somebody feel bad online are the same ones that may actually be reflected in the real world. Words hurt at the end of the day, and words matter, so what we say is really important.

DEVIN OLSEN: Cyberbullying is using technology to instigate harassment—targeted, antisocial behaviors. It's bullying through a screen, repetitively harassing people by sending negative messages, or posting unflattering or destructive information widespread online, especially in a closed situation like a school where everybody's going to know everybody at some level. Those are all examples of cyberbullying.

STEVE RYAN: Cyberbullying is any bullying that takes place over digital media, including text messages, social media, forums, chat rooms, and even video games and video game lobbies. You might see just one comment from someone, or there could be a pattern of cyberbullying.

JESSICA WALTERS: According to the National Cybersecurity Alliance, cyberbullying is a growing problem in schools, and teenagers and young adults are often the victims. What makes cyberbullying so harmful is how fast these messages and photos can spread. One rude comment can quickly spiral into several people piling on to antagonize a victim.

WHAT SHOULD STUDENTS DO WHEN THEY SEE CYBERBULLYING?

ALEX NETTE: My number one tip when you're potentially seeing or experiencing cyberbullying: If you are the victim of cyberbullying, ignore it. Block that person or remove them from your friend group. The interesting thing about your online identity is that you can see, hear, and respond to whatever you want. So if you're not interested in seeing or responding to something, don't and be done with it.

If you are seeing somebody else be the victim of cyberbullying, report it. A lot of social media accounts allow you the ability to report things that aren't working anymore for you in terms of what you want to see or when people aren't respecting the terms of service for that online social media account. The big idea here is that if

you can report it, ultimately that company can take action and potentially stop that or ban that user.

STEVE RYAN: The National Cybersecurity Alliance and StopBullying.gov have some great resources available online to help students, parents, teachers, and everywhere in between identify, prevent, and handle cyberbullying. Some recommendations that they call out is just don't engage with the bully. If someone's being rude or making negative comments about you or your friends, don't respond, ignore them, walk away from the laptop.

JESSICA WALTERS: Second, document the incident and report the account for bullying. Most social media platforms have community guidelines specifically that users aren't allowed to bully or harass others. If an account is reported for bullying, they might get temporarily or permanently banned from the platform.

Next, remove that person as a friend or a follower, or better yet, block them so they can't reach out to you again. You don't have to put up with negativity or rude comments. If you feel threatened, don't stay quiet. Report the incident to your parents, school counselor, or the local police.

ALEX NETTE: In all cases, though, make sure you tell a trusted adult what's going on. They can help you decide what to do next, or help you resolve the issue if blocking the person doesn't fix it. This can especially be the case if you do know that person in real life as well.

WHAT IS SOCIAL ENGINEERING?

ALEX NETTE: Social engineering is something that's been around as long as time, and the general idea is it is a con. In the old days, it might be playing a shell game on a street corner or getting hustled during a card game. These same scams and cons have been going on for hundreds of years. The only difference now is that they can happen online as well.

The other thing with these is that in the olden days, you had to be physically present to potentially fall for this scam. Now, somebody from hundreds if not thousands of miles away could also scam you. Social engineering, though, can happen in a couple different forms, whether it's emailing, which we call phishing; whether it's fake texts, which we call smishing; or fake calls that we call vishing—all of them potentially set you up to be a victim of a scam.

DEVIN OLSEN: Social engineering is a bad actor attempting to get your information by manipulating you into doing something—whether that's clicking on a link by sending you a message and that link will take you to a fake website that will steal the information that you log in with, or by convincing you to send them your information.

STEVE RYAN: Whether you're in elementary school or all the way through college or you're in the corporate world, everyone's heard of the "Nigerian prince" story, and that's a perfect example of some social engineering.

Social engineering happens when someone tries to deceive or manipulate you into giving them access to data they shouldn't have, such as your passwords, your bank account information, and things along that nature. For example, someone might send you an email or a private message saying they need to know your password in order to protect your Instagram account. Reminder: No website or app will ever ask for your password for them.

That type of social engineering is called phishing. This is spelled with a "ph," not the "f." So you can remember it by thinking about a hacker going "fishing" for your data. Those phishing emails can also include links to viruses, malware, or any other malicious files, as well.

Many phone-based scams also utilize social engineering. You might have heard of scams where someone calls a victim asking for money or gift cards. That's exactly the type of manipulation we're talking about here.

WHAT IS PHISHING AND WHAT SHOULD STUDENTS DO ABOUT IT?

LARRY KINKAID: Phishing is an element of "social engineering" is what we call it, but really it's a con through email. It is a fake email in which they want to either get something from you as the user—and I think nine times out of ten it's going to be a username and password, but they could just straight up be asking for iTunes gift cards. They could be just trying to gain your trust and pretending to be someone else, whether that's someone you already trust or someone that they find some credibility with. A common one's, "Hey, I'm the IRS. I need your Social Security number." If it's a phishing email, that's a con artist trying to gain access to your identity—your full blown identity outside your digital identity. Phishing is just a social engineering tactic to gain information from you or something that they want.

ALEX NETTE: Phishing at the end of the day is something we see a lot, and we often just attribute phishing as spam, generalized emails that we don't want. In fact, you may still be thinking that phishing is just for obscene or absurd schemes from a Nigerian prince. The trick today, though, is that phishing has evolved, and as a result, it ends up being much more tuned and tailored to you as an individual. So whether it's asking for a password reset, information about somebody you know, or even information about yourself, it can put you at risk. We also used to think about phishing as having weird misspellings or bad grammar, but with the advent of AI and things like Google Translate, all of those have gone away. So even if that phishing email is being set up by someone who's a non-native English speaker, as a result, it can actually look very believable and you may end up falling for it.

STEVE RYAN: Let's talk more about it. How do we identify those issues? Because as we know, every day it seems like I'm also getting texts, I'm getting emails from these random numbers or even random email addresses I've never interacted with. So how do we start to spot these phishing attempts?

Oftentimes, you can tell that email or DM is a phishing attempt by just looking at that message itself. After all, it's not very likely that the Instagram team would spell their own name—*Instagram*—wrong in an email to you. Finally, if you're on your desktop or laptop, you can also just try hovering over the link. If that link is saying, hey, this is a direct link to Instagram, and then you hover over that and that is not Instagram, that's a pretty clear indication that it's probably a phishing email.

What you should really do is first off, report that email. You want to report that to either your teacher or your school administrator. That way, they're able to tackle it and figure out maybe who sent that message, but also help protect future students from getting that message as well.

ALEX NETTE: What's interesting about phishing emails is they actually come in three different forms these days. The first is where it asks you to click on a link, whether that's resetting a password, clicking on a link to even unsubscribe, or potentially clicking on something to check an alert that you've received from a website, all of them could get you to try to click on that link.

The second way, though, that phishing ends up happening is there might be an attachment. Unfortunately, often that attachment is malicious—and so what it says it is, isn't what it actually is. So maybe there's a receipt attached or it says, hey, can you check out this Word document for

review? That could be a way that ultimately malware could get installed on your computer.

The final is what's called a form fill. And oftentimes this means that the email might not be the phishing part. So you might click on a link, you may go to a webpage where it says log in with your Google credentials. That webpage, though, isn't actually Google—it's a fake site. As soon as you type in your information, it captures it, and that hacker or scammer can use that information.

All three of those are equally dangerous. The number one recommendation to avoid all of these, though, whether it's sending potentially a receipt attached to your email, asking you to fill out an online subscription form, or log in with your credentials, or click on a link to check an alert is to go directly to the website. Don't click on the link in the email. Go directly to the website that you know and trust and check if there's anything there for you to look at. If there isn't, that email was probably a phishing email.

WHAT ELSE CAN STUDENTS DO TO HELP KEEP THEIR PERSONAL INFORMATION SAFE ONLINE?

ALEX NETTE: My number one recommendation is the information that you share is the information that you have to keep safe. The second one, of course, is limiting who has access to your information. Be careful who you're friends with online and definitely be sure not to reuse passwords. Use complex passwords and use different passwords on every single account that you have online. If you use the same password for every app, a hacker only needs to figure out one password in order to gain access to multiple accounts that you own or manage. That means that the password that you use on Facebook could end up being the way that a hacker drains your bank account on your bank website. By mixing it up, you significantly lower your risk of being hacked across several websites at the same time.

The second tip—and it marries right up with this—is to turn on multi-factor authentication, sometimes called 2FA or MFA. If you've ever had to type in a code after inputting your username and password, whether you receive that code via email, a text message, or some sort of app, you know what I'm talking about.

MFA ultimately keeps you safer because once you turn it on, even if a hacker has your password, they still can't get into your account. It's a great way to add that extra layer of security. Another way that we can do this, too, is to think about an alternative form of authentication, like Touch ID or Face ID on your Apple devices. Just make sure that if you use these, you still have a strong and secure password set as well.

STEVE RYAN: Don't click on those suspicious links in an email. If you get an email that you're not familiar with and it's embedded with links, just ask. Check with your teacher or another trusted adult if you receive any of these weird messages.

And finally, don't overshare private information and especially your passwords online. Set your social media profiles to private, consider leaving things like your school and last name off your profile altogether. Really, all these do is allow an attacker to gain more information about you, to have a more direct and potentially more customized way of talking to you, to make them feel more real even when they're a malicious person.

TALKING POINTS

Episode 4: Cyber Hygiene

WHERE DOES YOUR DATA LIVE?

"Our healthcare information's online. For a student, your grades actually are now online and accessible remotely. Certainly, stuff like your bank accounts, one day you might have trading accounts or stock market accounts, those types of things. All of that information is accessible, if not only by you, it's accessible by anybody who might be malicious and want to try to access your account. So using proper cyber hygiene is really important."

—Daniel Colgrove, Broadleaf Commerce

CREATE UNIQUE PASSWORDS

"Reusing passwords makes a hacker's job easier because they only need to figure out one of your passwords in order to hack into several of your accounts. Create a unique password for each account you have so that if one is compromised, the damage is limited to just that one account."

—Devin Olsen, BARR Advisory

CONTINUE THE CONVERSATION:

- **What are some of the risks associated with using the same password for multiple accounts?**
- **What is multi-factor authentication (MFA) and why is it so important?**
- **How can you tell if an email you receive is a phishing attempt?**
- **Your friend keeps a list of all their passwords in the Notes app on their iPhone. What would you say to them to convince them to change this practice?**
- **Should school districts require students to use MFA to log into their school accounts? Why or why not?**

TRANSCRIPT

Episode 4: Cyber Hygiene

WHAT IS CYBER HYGIENE?

DANIEL COLGROVE: Cyber hygiene, really, is trying to keep you, yourself, your personal information safe and secure online by using strong passwords and just making sure that people aren't somehow hacking or getting into your accounts because of having passwords that aren't unique or complex or strong in nature.

COREY EMERSON: Making sure that you have the right information out on the internet—and by that, it's as little as possible. There are data brokers that gather and scrape across our social media accounts, and then they sell that data to advertisers or groups. Anybody with a checkbook can buy demographic data from data aggregators. We can submit requests to these data aggregators to remove our data, but the best thing to do is to have as little data available to these people and to these groups as possible, because it's not always advertisers who are looking at our data.

DEVIN OLSEN: The term cyber hygiene encompasses all the steps that you take to keep yourself and your personal information safe and secure online. This includes things like creating unique and complex passwords for all of your accounts and keeping those passwords safe from hackers and from wandering eyes.

WHY IS IT SO IMPORTANT TO CREATE SECURE PASSWORDS?

COREY EMERSON: A student is at the start of their life. My worst password when I was a kid was the name of my cat and then the year I was born. And I thought that was great, but I used it on everything. And so all it takes is for one site you sign up for to have your password stored incorrectly to pop all of your accounts.

DANIEL COLGROVE: These days, your life is online, right? And your information is available, readily available out there. And having a strong password is really key so that people can't get to that. If somebody were to steal your password and get access to an account, right away, they've basically stolen your identity. They have access to your accounts. They even can get to the point where they can impersonate you. And I've seen that, I've received emails from friends and it's, "Hold on a second, this email doesn't seem at all like my friend." And I've reached out to him and they're like, "Oh, yeah, sorry. My email has been hacked." And if I wasn't astute in recognizing that something's not quite right, they could have easily asked me for help, assistance, money, whatever it might be. So it's really key, especially these days since we live so much online, that we have proper passwords in place.

If you think about it, how much of your data is online? Our healthcare information's online. For a student, your grades actually are now online and accessible remotely. Certainly, stuff like your bank accounts, one day you might have trading accounts or stock market accounts, those types of things. All of that information is accessible, if not only by you, it's accessible by anybody who might be malicious and want to try to access your account. So using proper cyber hygiene is really important because of these types of things.

DEVIN OLSEN: Most commonly, when we're thinking about stolen passwords, we're thinking of identity theft. So when someone uses a stolen password to access your account, they could gain access to sensitive information, like your grades, your health records, or even your bank account numbers.

There's also the risk of losing access to your own social media accounts. For example, a hacker could get into your account and change the password, preventing you from accessing your messages and followers and photos. Practicing good cyber hygiene is a great way to prevent this from happening. That's why it's so important to create secure, unique passwords for every account you have.

COREY EMERSON: With enough details, people can open up lines of credit. A strategy that lots of parents do for their kids, and some people agree with this and some people don't, is that when their kid's in high school, they'll open up a credit card in their name. So, there's nothing stopping anybody who has enough details on you to just open up a credit card in your name. And they're not going to have the same intention as your parent.

WHAT ARE SOME PROVEN TIPS FOR CREATING SECURE PASSWORDS?

DEVIN OLSEN: The first is to never use the same password twice. Reusing passwords makes a hacker's job easier because they only need to figure out one of your passwords in order to hack into several of your accounts. Create a unique password for each account you have so that if one is compromised, the damage is limited to just that one account.

The next is to use a mix of letters, numbers, and symbols. The more characters, the better, strictly speaking. But don't use recognizable phrases or numbers that are significant to you or easy to guess, like your birthday—bad idea. In fact, the best password is actually a passphrase. By stringing a bunch of words together, you can create a very long password that's extremely hard for hackers to guess. The most defining characteristic of a secure password is the length of the password. A good passphrase includes five to ten words of nonsense. The words should all be unrelated to one another and it shouldn't sound like a sentence. You can even put spaces in between the words to make the password even longer.

Using a password manager to keep track of all those different passwords is another useful tool. Between social media, school accounts, work accounts, and more, you might already have way more passwords than you can remember. It can be really tempting to write them all down or put them in a Google Doc, but that's not very secure. All someone needs to do is see that paper or Google Doc and suddenly they can access all of your accounts. A password management tool can help you keep everything straight by storing your passwords for you behind one single "master password." That way, you only have to remember one password—and since you don't have to remember all of your passwords, you can make them that much more complex and harder for cyber criminals to crack.

DANIEL COLGROVE: When you create your password, it's a good idea to use a mix of letters, of numbers, of special characters, and when you use some of those, also be conscious not to use personal information. For example, if you use numbers, don't use your birth year, or maybe don't use your full birth date. It's just stuff that's public information already, and hackers, that's a common tool for them to try to figure out, maybe try to use a variation of a birthday.

Also, the longer the password, the better. I think today, they typically recommend 12 to 16 characters. I know that seems like a lot. One technique that you could try to use to manage longer passwords like that is use what they call passphrases. Passphrases are just a series of words that are strung together. They're random words. And you can just come up with some words that probably make sense to you in some type of a context. But when you read them, they don't necessarily make a lot of sense. They don't form a sentence of any kind, but if you put together four or five, six words like this, before you know it, you'll have 12 to 16 characters or more. And it's a lot stronger to do that.

And for sure, as we get into these longer passwords, don't write them down. That's easy to do to help me remember it, but don't write it down and certainly don't post it in some type of a document that maybe you have online if you use some form of Google Documents or something like that. Don't keep them online like that either.

And you might ask, okay, if I can't write them down and they're long passwords, what do I do? There's password managers that are available. Some common ones are LastPass, OnePass is another one. A lot of times they have them on your phone or you can put them on your laptop or desktop, and they're specifically designed to store your passwords and then to make sure that only you have access to it. You'll create one master password that allows you to access that, and obviously you want that master password to be more complex as well, but you only have to remember that one. And then from there, you'll go into the password manager, you'll get your password, and then you can use it on your account.

COREY EMERSON: Before you select one, make sure you do your research—because you absolutely don't want to pick one that's been in the news repeatedly. And from there, you only have to do one password. When it comes to creating a strong password, the longer a password is, the better it is, because to brute force it, they have to do every character back to back. So if you say, pick your favorite song lyric, right? And you maybe replace two of the letters in that song lyric with numbers and then have a symbol somewhere in it, that is going to be the strongest password that you can have. And then that's just the password to your vault, and it creates the rest of them.

Additionally, you're going to want to set up MFA using any MFA app. Try to make sure it's from a reputable source. Microsoft has one. Google's got one. There's Authy. Some of the password managers also have MFA.

WHAT IS MULTI-FACTOR AUTHENTICATION (MFA) AND WHY IS IT SO IMPORTANT?

DANIEL COLGROVE: That's a good question. So if you've ever been to a site and you typed in your username and password and then you've been prompted for one additional piece of data, that is the multi-factor. It's easy to pass out your password, and people might have your password, but that extra piece of information, they most likely won't have. And that's the whole point—it just raises the security bar. And typically it's going to be, your password will be one that you'll want—so it's username and password—and then a lot of times, you'll get some type of maybe a notification through a text or via email for that second piece of information.

There's also one where you can get what's called an authenticator application. You would typically put it on your phone and it'll prompt you for, "Hey, give me the number from your authenticator application." And so you just pull that up on your phone. It's actually time-synced, and so every 30 seconds, it generates a new code. And that's synced as well with your provider, whoever you're trying to log in with. They have a sync process too. So you would look it up and you'd say, okay, the code is "123," you'd go to the application, you type in "123," and it would allow you to log in.

And then the last one is it could just be a function of using the Touch ID or maybe your facial identification to get into the account as well. So multi-factor is using more than one, it's using multiple data points about you, so this makes it much harder for anybody who's trying to hack in—bad actors is what we call them—to try to get access to your account.

JESSICA WALTERS: MFA is a way for you to prove that you are you. So whether you're logging into your email from a new device that maybe Google doesn't recognize and they want to make

sure that it's you and it's not someone pretending to be you, they can give you a second factor to prove that it's you. Some ways you may see this happening is you may have a code sent to your phone and then Google will ask you to input that code, or they might ask you to open up your app on your iPhone that they see you're logged into to prove that it's you logging in somewhere else. These are all ways that are designed to keep you safe.

COREY EMERSON: Authentication and identity comes down to concepts, right? A password is something I *know*. A multi-factor authentication method is something I *have*. A fingerprint is something that I *am*. The more layers that are different that we can add to our authentication to sign in to anything on the internet, the harder it is for anybody to impersonate us.

DEVIN OLSEN: If you've ever had to type in a code after inputting your username and password to log into a website, then you've already dealt with MFA before. When you enable MFA, it will take two or more steps to successfully log into your account, so to log in, you'll have to verify your identity with at least two of these three things. And this makes it much tougher for bad actors to gain access to your accounts, because they'll need a lot more than just your password to get in.

HOW CAN STUDENTS SET UP MFA FOR THEIR OWN ACCOUNTS?

DANIEL COLGROVE: Whoever you're using—your social media account, your bank account—they have to support MFA, and most of them will. These days it's become a very standard practice to have that extra layer of security, and so typically what you would do is you'd go to your profile or go to the settings—once you've logged in, go to the settings of your account—and then there typically would be a section called security or maybe it's called privacy, and you can go in there then and just enable that multi-factor authentication.

I mentioned that authenticator application, a lot of times what they'll do then is they'll step you right through the process. They might give you a QR code, which you've seen that—it's a block barcode, and you would scan that code in with your phone, and that's that sync process I mentioned that you would use. So they'll step you right through that process, but you'll be able to get it set up. And just know too that when you have MFA, there's a few extra steps that you have to take to get logged in, which, to some degree you might [say], "Man, that's a bit of a hassle for me to do that." But if it's a little bit of a hassle for you, it's a big hassle for people who are trying to hack in, right? And if there's a multi-factor authentication, a lot of times they're not even interested in trying to hack that. It's too tough. And so it's a good layer of security for yourself.

DEVIN OLSEN: For most apps, you'll go to the settings and click on either privacy or security, and from there you should be able to turn on two-factor or multi-factor authentication, however it's listed. It may take a few extra seconds to log in, but the security benefits make it well worth your time.

ARE THERE ANY ONLINE SCAMS THAT AFFECT STUDENTS?

COREY EMERSON: A common thing that happens, a common tactic by scamming people on the internet, is a concept called social engineering. If I wanted to do a social engineering attack on an organization, a person, whatever, I would try to learn about that person, try to learn who they're friends with. If their profile is public on Facebook or Instagram, I would go look and I would see what kind of places they visit, what kind of pictures they post, what kind of things they do. If I know your phone carrier, and I knew which bank you went to from posts, I could try to impersonate you.

A lot of financial institutions are behind the times, and they only offer MFA via SMS, like a

text message. The reason that's not super secure is because you can do an attack, as someone trying to do something bad on the internet, that basically takes your phone number and applies it to somebody else's phone through calling your phone provider and trying to convince them that they're you, and say, "Hey, I lost my phone. I just got a new number. Here's the SIM." That has happened, where all of a sudden your phone doesn't work. And it's because somebody just put your phone number on their phone. If they're convincing enough, that can happen to anyone.

DANIEL COLGROVE: And you probably see these all the time, if you're online and have an email, even as a middle school or high school student, you're going to see emails that appear to be coming from a legitimate source, but they're not. This is actually called phishing. It's an email, it's a text message, it's a phone call, and it's really somebody who's trying to act like they're coming from a valid source. They're being manipulative in the process, but they're not legitimate at all.

So, if you get an email, if you look at that email, you might notice that the English seems a little bit off or there's typos in the email. And so there are clues that definitely tell you that something's not quite right here. But probably the most important part of that is at the end of the day, they're trying to get you to click a link, and that link is going to take you somewhere that you don't want to go. And as you mouse over your link that you get sent via email, you can see in the status bar of your browser what that link is actually going to, where it's going to. And if you look at that URL, it's not going to be what you would expect. It's not going to be the name of the bank or the name of whatever entity you're trying to go to. Keep an eye on that, because that's really the final piece—hey, is this link even real? And so you'll notice if you look closely, it won't be.

So if you don't know 100 percent that link is going to a legitimate source, don't click it. That's the best advice is just don't even go to it. And in most cases, I would just delete that email. You can also report it to somebody like a teacher if you're in class or even your parents, they can verify that as well.

This is more and more common, and I'll tell you, over the years that I've been involved in this industry, the emails have gotten more sophisticated. And so I've seen emails that I'm double-guessing myself, like, is this real? And like I mentioned, going and looking at that link is probably the final piece that you want to look at—is this really going to go take me to the place I would expect? So just be on your toes. People are getting more and more clever these days on how they can try to get your information.

DEVIN OLSEN: They collect where you work, who you're friends with, what your browsing habits are. All of those personalized ads are getting that information from all of these websites that are selling your information online. So anything that you do online becomes part of this information packet that makes up you, your digital footprint, and that can be sold by just about anybody. If you ever really want to take a good look at what an app is collecting, go and look at the permission sets for Facebook Messenger, and it will tell you everything that it is allowed to touch on your phone. And it is quite a significant list.

COREY EMERSON: A major component of a phishing attack is a call to urgency, so if ever you get a message and they're trying to get you to react quickly and not think, just do. An example of a phishing attack that happens all too common is a grandparent will get a phone call or an email saying that their grandchild is in jail and they'll need to post bond. And so without even calling their grandchild to verify or their parent, they just send money.

DEVIN OLSEN: You might get an email or text message asking you to click a link and input your password or student ID number, for example. Oftentimes, these emails have typos or grammatical mistakes in the message or in the sender's email address that look suspicious. So if anything looks off in an email you receive, take a closer look. Are simple words misspelled? Did they type an O where there should have been a zero? Don't click on any links in emails until you're absolutely certain it's coming from a legitimate source. And if you think an email is a phishing attempt, or you're not sure, report it to your teacher or another trusted adult.

WHAT ELSE SHOULD STUDENTS DO TO PROTECT THEMSELVES ONLINE?

DEVIN OLSEN: To protect yourselves, reading *everything*. I know it's really easy to just click through and click "accept" without checking all the details, but it is a good idea to actively pay attention to what these things are collecting, what they're accessing, what they're touching across your devices and your accounts.

As far as my personal opinions on it, I believe that we lack digital privacy. There are applications that you can use, like VPNs. A VPN is a virtual private network. Essentially, it means that it hides the IP address from which you are connecting to the internet by filtering it through a series of other IP addresses that it has access to and obfuscating or hiding where you are connecting from. It doesn't stop things from tracking what you're downloading or things like that or cookies, but it will help prevent tools online from absolutely locating your location, which is most certainly an easy and accessible thing for a great many programs to do.

DANIEL COLGROVE: I think something that people don't necessarily think about is, when they're out and about doing their daily chores and activities, whatever it might be, when you get on your phone and you connect to a WiFi spot, whether it be a Starbucks or some type of venue where you're at, you want to be really careful that network is as secure as it can possibly be.

There's a lot of public WiFi networks that are just too open, they're too exposed, and, to a large degree, you don't know exactly who they are. If you see a name when you go to connect to a network, that name is set by somebody—it could be anything, right? Here in my house, I could actually set a WiFi name of Starbucks, and that gets broadcast out and somebody could connect to it thinking, "Hey, there's a Starbucks WiFi." And so don't trust the name of the WiFi that you see. It could just be open.

More importantly, what you really should do is if you're at an establishment, and they do provide WiFi, you want to confirm the name. In most of those places, they actually should have a passcode, and so that then restricts who has access to it based on the knowledge of that passcode. That would help as well, making sure that you're on a legitimate network. And then worst case, if you're not sure, you can use your own hotspot from your cell phone, and that might be a good way. At least you know the network you're on is your cell phone provider's network. That's just another component that people don't necessarily think about, but that's definitely a good way to continue to protect yourself online.

DEVIN OLSEN: I would say that reducing your cyber footprint, minimizing the number of websites that you are giving your personal information to, minimizing the number of places that you are sharing your personal information on, is probably one of the best digitally aware skills or practices that you can engage in for the rest of your life. Your digital footprint is your existence in cyberspace. It's all of the websites that you have stored your information on, all the places that you visit—anywhere that you touch online becomes part of your digital footprint. The larger it is, the easier it is for people to find you, to find your information, and then to get access, opening up more surface area for them to attack. If you don't have to add your information to a place, I would recommend that you don't.

The other one is I would recommend occasionally checking websites that monitor whether passwords or accounts have been leaked online. The most common one is *haveibeenpwned.com*. That will check your information against a database to see if your information, your accounts, your passwords have been leaked and stored in all of these innumerable files that have been distributed across the dark web. And that will help you to ensure that you are maintaining good cyber hygiene.

TALKING POINTS

Episode 5: Future of Cybersecurity

CYBERSECURITY IS FOR EVERYONE

"You lock your car, you lock your locker, you protect things that you own. And your digital identity is one of those things that you should own and protect."

—Larry Kinkaid, BARR Advisory

AI CAN BE A USEFUL TOOL...

"Those that are acting nefariously will be creative, and so AI will help us make sure we're covering all the different possibilities and areas we need to keep things safe."

—Balaji Gopalan, MedStack

...BUT USE AI RESPONSIBLY

"You, as a student, as a creative person, can write something much better than ChatGPT ever could. ChatGPT is a starting point. It is not your ending point."

—Keri Barnett-Howell, Mission Cloud

CONTINUE THE CONVERSATION:

- **Cybersecurity is everyone's responsibility. Do you agree with this statement? Why or why not?**
- **Why is it so important for companies to be transparent about issues related to cybersecurity?**
- **How might new developments in technology and artificial intelligence (AI) benefit the cybersecurity industry?**
- **In what ways might new technologies like AI cause challenges for cybersecurity professionals?**
- **What are some strategies you could use to verify that the information you find online is accurate?**

TRANSCRIPT

Episode 5: Future of Cybersecurity

AT ITS MOST BASIC LEVEL, WHAT IS CYBERSECURITY?

BALAJI GOPALAN: What is cybersecurity? Cybersecurity is the topic of keeping data safe. Now, that's data and everything that runs in it. So think of all of the technology within the internet, like websites and apps and devices and other things we might use—including the hardware that actually transmits the data into our houses, for example—all of that falls into the realm of cybersecurity. The work to keep that data safe and those technologies safe is what allows us to trust that we can actually use them.

There's lots of different kinds of roles in the world of cybersecurity. There might be people who do the work of building safeguards and securities within certain companies, whether that's things they use internally or things they use for their customers. There might be people who are literally paid to figure out whether another company is doing things safely so that we know we can trust them. And there's other people that are actually in the space of testing those things to make sure we can maybe find out things that are at risk that we didn't actually think of before. All of this falls into the realm of cybersecurity, which is really driving trust.

LARRY KINKAID: Funny you ask. Cybersecurity is a very broad, very all-encompassing term, because there's so many subdisciplines that build into cybersecurity. You've got analysts, you've got engineers, you've got auditors, there's even people that are paid to hack into other people's systems. Cybersecurity as a whole, there's a lot of meat within that term.

BALAJI GOPALAN: In today's world, cybersecurity is very broad. Anything we do to protect data, networks, websites, and systems from unauthorized access falls under the umbrella of cybersecurity.

KERI BARNETT-HOWELL: Cybersecurity is the practices of keeping individuals and companies safe on the internet. Since the internet has been created, people have been trying to get data, do cyberattacks, things like that, get through firewalls—all these kinds of things you may not know the words of, but it's how we keep the internet safe for people to use and companies to use.

Every time you type something into the internet and it gets saved somewhere, you don't really want people looking at that. You don't want people seeing what you've put in there, and so cybersecurity is the industry that has been created to figure out: How do we keep everyone safe?

BALAJI GOPALAN: Some people work as cybersecurity consultants. They might tell CEOs, for example, and other cybersecurity specialists, how to protect their company's data.

KERI BARNETT-HOWELL: Others work as auditors, checking to make sure that companies are actually doing what they say they're doing to keep their customers' data out of the wrong hands. Some people even get paid to try to hack into companies' systems so they can identify weaknesses before the real hackers do.

IN 2023, IS CYBERSECURITY SOMETHING EVERYONE SHOULD BE INVOLVED IN? WHY AND HOW?

LARRY KINKAID: Of course. Just considering how, just in general, the internet is more than

just business, right? We all use it for a lot of personal use cases. Essentially, it's an asset just like anything else would be. You lock your car, you lock your locker, you protect things that you own. And your digital identity is one of those things that you should own and protect. The good thing is that you're likely already doing a lot of things well. Obviously, passwords are something that we should protect and ensure are strong, and the good thing about that is the longer, the better. Complexity also plays a factor, but the more characters you have in there and the longer it is, typically the more secure it is.

Another thing that's becoming more and more accessible on a personal use case level is password managers. What is happening is, hackers know that people reuse their passwords or somehow iterate off the same password. So when you use a password for an account that you've made two, three years ago and completely forgot about it and that company gets hacked and you don't even remember making an account there, they're going to take these usernames and passwords and plug them in and then try to get as much as they can out of it, whether it's your social media, your Netflix, or even your bank accounts. So password reuse is a huge problem. That's where password managers come into play. If you remember one strong, robust, long password, and then within that vault or that safe, that manager, you then use a bunch of random characters or passwords that you don't even know to your various systems, such as your bank accounts, your social media, that's where you get the protection that you need. Because if that password is compromised for that one-off account, it doesn't then compromise the rest of your digital identity.

BALAJI GOPALAN: Absolutely, yes. Anybody who spends time with digital data on the internet through websites or apps or other things needs to know and be comfortable with the notion of cybersecurity so they can trust the things that they're working with. And there's things that we are all involved in when it comes to cybersecurity. Some things are basic, we all know them. For example, a lot of things require a password, and you need to think about what makes a good password. You wouldn't put in the word "password" for your password, or your birthday or your name. You want to come up with something that maybe other people can't guess. That's the first step towards cybersecurity. When I'm talking to students, I'm looking to expand their knowledge and awareness of why these things are important, for example, what makes a good password. To talk about that, for example, you want to make sure that you have a password that other people can't figure out, that maybe is a little bit long. You want to make sure you're not using the same password in multiple different places.

One thing that we recommend to actually manage this is the notion of a password keeper or a password manager. These are things that might be built into your web browser or into your phone or an app that you download that allows the system to create complicated passwords for things, but you don't actually need to remember what any of them are. You just need to remember the password for the password manager, which might then be supplemented by things we all know as other ways of authenticating, like a fingerprint, or a picture of your face, for example. These are the first steps towards cybersecurity, and it involves everybody, not just people who actually work in these roles.

KERI BARNETT-HOWELL: Anyone who spends time on the internet should know and be comfortable with the basics of cybersecurity. So you are probably already familiar with a lot of the things that we do to keep people safe. For example, your password should not be password123. My goal in speaking with you is to expand on that knowledge. You can think about things like making a stronger password can really help with security.

BALAJI GOPALAN: At the most basic level, the answer is more characters. The longer your

password is, the longer it will take for hackers to figure it out. That's why so many cybersecurity professionals nowadays suggest that students and employees use passphrases instead. That is, create a nonsensical phrase of unrelated words like book-giraffe-jumping-ladder-with-helicopter, something you might remember. Putting spaces between those words can also make your password even longer.

KERI BARNETT-HOWELL: Another tip I've learned during my career in cybersecurity that I think everyone should follow is using a password manager to keep track of all your passwords. It's a bad idea to use the same password for multiple accounts because then, once a hacker has access to one account, they'll have access to all of them. It can be challenging to keep up with dozens of passwords, especially if they're as long as they should be, so using a password management tool like Google Passwords can help you stay organized and safe.

IN YOUR EYES, WHAT ARE SOME OF THE BIGGEST RECENT DEVELOPMENTS IN CYBERSECURITY?

BALAJI GOPALAN: There's a lot, but one of the most important is the notion of transparency. Cybersecurity, because so many of us are talking about it, it's become an important topic, and it's important for companies to show that they take it seriously. We've met a lot of people, those of us who are working in this career, who have really shifted towards this notion of being open and honest about cybersecurity, because it helps all of us do it better and grow and learn.

So you'll find more often now, companies are actually being upfront about the notion that they might have discovered that there's a problem that they have to address or that there was a hack, rather than hiding it, which is maybe something that might have happened before, and this is really good for the whole industry. At the same time, when people know they've been affected by a hack, they can take steps to protect themselves.

LARRY KINKAID: It's interesting to see the evolution of cybersecurity over the past decade. The cool thing is that there's a lot more transparency, a lot more of a community, and a network in which people are helping each other. Before it would be a lot of, "I don't want to show my cards, I don't want to show my skeletons in my closet," but even with more recent breaches or hacks that we've seen, there's a lot of transparency and a lot of lessons learned that the community can then apply to themselves, so that's been a really cool thing.

Automation has been a huge development as well. With the ever-growing footprint that we have on the internet and with our digital identities, the idea before was like, alright, we have one person doing it, now we need two, now we need three, and we just need to continually grow our department as we're ingesting more and more data. The idea of automation allows us to essentially have more time and resources spent on solving issues than finding the issues, which has been really cool.

And then in addition to that, of course, AI. I look at AI as a disruptor and a game-changer that needs to be embraced, but also needs to be managed. There's a lot of risk associated with it. There's a lot of problems that can come out of AI. But I think that if we treat it the right way and understand it and then leverage it in the right ways, it can be a really powerful tool.
So disruption is something that's introduced into an industry that will change the game. It's something that may not have been there before, and now with the introduction of it, the playing field is completely different. One could say the forward pass in football was a disrupter. The three-point line in basketball. I'm a big fan of sports analogies, but Nest was a disrupter in the thermostat space. Technically, TikTok was a

disruptor for Meta. Twitter was actually probably the original disruptor within social media. But the point being that these disruptors are things that when introduced into a space, it really changes the way we have to think about it.

KERI BARNETT-HOWELL: One of the most important trends I've seen is more honesty from cybersecurity professionals and companies. Most people that I've met throughout my career care a lot about being open and honest about cyber-security, because it helps us all grow and learn. For example, when companies tell the truth about being hit by a cyberattack, we can learn from their mistakes and try to prevent them in the future. At the same time, when people know that they've been affected by a cyberattack, then they can take steps to protect themselves.

Earlier in 2023, the U. S. Securities and Exchange Commission, also known as the SEC, published new rules for public companies saying they have to tell the public about significant cyberattacks and breaches within four business days. This is a great step in the right direction, and I expect other governments will soon follow suit.

BALAJI GOPALAN: Another trend that's helping companies improve their cybersecurity is automation. Developers and cybersecurity experts have created software and tools that make it easier to ensure that everyone is doing what they need to in order to stay safe. The cybersecurity industry is also getting started in figuring out how artificial intelligence, or AI, can help keep organizations and individuals safe.

WHAT ROLE WILL AUTOMATION PLAY IN THE FUTURE OF CYBERSECURITY?

KERI BARNETT-HOWELL: This is a huge question that we tackle a lot in cloud industries. Automation is massively important, because there's just no way that individual people can keep up with all of the security needs that companies across the globe will need to keep themselves safe, especially from new attacks using AI. So for businesses, automation tools make it easier to monitor their networks for cyberattacks and ensure only the correct employees have access to sensitive information and data. Automation tools can also help businesses keep up with changing laws and regulations surrounding cybersecurity.

BALAJI GOPALAN: And for individuals, this means companies have an easier time keeping your data secure, and they can do a better job of holding themselves accountable if and when a data breach does occur.

LARRY KINKAID: Automation will make things easier. It'll allow us to scale, and when I say scale, it essentially means that we can do more with less. Automation will give us back our most valuable resource, which is time. A great analogy there would be finding a needle in a haystack. We could spend eight hours finding a needle in a haystack, or we can leverage automation to find that needle. So then we have the rest of the eight hours to determine: Is it a needle? Is the tool working? And what do I do with this needle? And that saves, again, time, which is money in business especially, but then it allows us to focus and be more strategic and use more of our critical thinking as opposed to spending most of our time spinning our wheels, trying to find the problem.

And then take that whole use case and just take it through all the disciplines of cybersecurity. Automation is a very powerful thing that we need in cybersecurity. Another terminology we like to use in cybersecurity is "noise." There's a ton of noise and we have to sift through that noise. Automation is the noise-canceling element, right? We get to focus and hone in on the thing that we're looking for, instead of wasting time, money, and resources on just trying to find that issue.

HOW WILL AI PLAY A ROLE IN THE FUTURE OF CYBERSECURITY?

LARRY KINKAID: I think this is a very interesting topic just because with a new tool, with a disruptor like generative AI, ChatGPT, Bard, there's of course the element of abuse—having the AI write your papers for you, and obviously that is unethical and creates more of a concern on missing the point of the assignment, if you will.

But with that being said, I don't think that AI should be completely ignored, either. It's a great starting point. It's a great idea generator. It's a great brainstorming tool. It's a great research tool. But I think people need to understand that AI is not infallible. It's not something that should be just used in a vacuum. And obviously understood in the sense that proper research still needs to be done. I think the same thing happened with Google as well; people were Googling things and copy and pasting from articles without proper references and checks on that, the same thing needs to be treated with AI. But it should still be used and can be leveraged, because I think that the way that it needs to be looked at is AI is a tool. And with that, the way we use it is going to be a skillset that's going to be really valuable in the future. So the people who can know how to Google really well and get to what they're looking for really quickly, it's going to be the same thing with AI.

KERI BARNETT-HOWELL: So for cloud industries, AI is going to play a huge role in the future of cybersecurity, because it will work hand in hand with automation tools to simplify how we build the infrastructure of the internet. When we build infrastructure, we have to spend a lot of time figuring out how to keep companies' data safe. If we could automate that process, it would make everything faster and cheaper. AI tools can help cybersecurity professionals recognize patterns and make it clear when something has gone wrong.

And I have to say, there is no job that you're going to go into in the future that will not include AI. In my role and all of the roles at my company, we are already starting to use artificial intelligence for all of our daily tasks.

LARRY KINKAID: Just like we need to think about it in a sense of education, it's also something that we can leverage as a tool within cybersecurity. Something that I've seen that I thought was really fascinating is in cybersecurity, we have this term called "indicator of compromise." And all that is, is it's a way of communicating between a bunch of different resources to say, "This is what you need to look for in your network to know this is a problem." But that's the thing, right? Hackers know, "Hey, I need to change things up so I can fly under the radar so you can't find me." So indicators of compromise can change and adjust and evolve. AI can help us think through that, "Okay, here's this indicator of compromise, what are other iterations of that indicator?"

There's also different ways on the alternative side of phishing emails. Before, phishing was a very easy thing to look at and say, "Oh, that's a phishing email because of the sender, the subject, the grammatical errors, the URL." AI will help eliminate grammatical errors and essentially create better phishing campaigns. That's a scary thing, I think, on our side, but good comes with the bad when it comes to the disruptors like AI.

BALAJI GOPALAN: Those that are acting nefariously will be creative, and so AI will help us make sure we're covering all the different possibilities and areas we need to keep things safe. Some AI tools can also help detect and even prevent cybersecurity threats by monitoring user activity and automatically blocking unauthorized attempts to access secret or confidential data. As generative AI tools become more accurate and sophisticated, we might see young people who are students today working in roles that encompass both AI and cybersecurity in the near future. If you're thinking of going into

tech or cybersecurity, you have a lot to look forward to. It's an exciting field and new developments are popping up every day.

KERI BARNETT-HOWELL: I definitely want to emphasize that it is a very good idea to familiarize yourself with all of the AI tools. It's a great idea to sit down with your teacher or your parents and go through the tools together. What can you find out together? Recently, my husband and my kid, we sat down and we planned a vacation using ChatGPT. It was such a cool tool to use to figure out: What have other people done? What activities have they found? And it was really fun to play with. So these tools are not scary, they're fun. You're going to need to know how to use them. They're going to be a part of your future career. But it's a good idea to learn what the capabilities are and where the limits of their knowledge are so you can keep yourself safe and you can keep your family and any company you might work for safe.

ARE THERE RESPONSIBLE WAYS TO USE GENERATIVE AI TOOLS? WHAT ARE THE RISKS AND BENEFITS?

BALAJI GOPALAN: In many ways, we're still figuring out the best ways to use generative AI tools like ChatGPT, and the tools aren't perfect. They might give answers that sound convincing—they're meant to sound conversational. It is well-known they might sometimes get the facts wrong, and it might mix things up altogether. This is why at many schools, there's actually policies against using tools like this, including at my kid's school. So if you're if you want to use a tool like this, first of all, make sure that you follow the student handbook, or ask your teacher for clarification if there's guidance on how you can use AI tools like this.

And there's lots of sources of information, even in the world that existed before generative AI that we do know have factual backgrounds. But depending on the situation, a tool like ChatGPT or other generative AI tools has a use, and it's great for a creative starting point, so if you're thinking about brainstorming or trying to put different ideas together to creatively come up with an inspiration for something, it works very well for something like that. But you should never ask the system to write an essay for you. It's a partner in brainstorming. Getting it to write it for you would always be a bad idea and actually get you in trouble as your educational career progresses. Also remember that while these tools are powerful that you can actually use, there are also other tools that are now being developed to detect that you're actually using them. So keep that in mind and use them responsibly and transparently.

LARRY KINKAID: We definitely don't want to see ChatGPT cranking out essays that you copy and paste into your Word docs and hand off to your teachers. But ChatGPT and generative AI, conversational AI in general, is a very powerful tool that if used in the correct way can enrich your papers. It creates benefits in the way that you can use it for brainstorming or as a starting point. But with that, as with anything, ChatGPT, Google—they're not infallible. They're not always right. There's this idea of "hallucinations" is what they call it within AI, because there's biases, there's a certain misinformation that can be portrayed. That's why even with generative AI, you would want to do reference checks and verify your findings. Nothing will ever beat a true reference check on something that's credible. ChatGPT in and of itself is not credible, but again, it's a tool, and I think that the skillset in leveraging that tool will be something that's extremely valuable in the future. I know in cybersecurity, people that know how to use AI and also know cybersecurity are very valuable in our field. And not only are you doing a dis-service to yourself by using ChatGPT to do your essays, but there's going to be more and more tools and more discovery tactics to sniff that stuff out.

KERI BARNETT-HOWELL: We're still figuring out the best uses for tools like ChatGPT. These tools aren't perfect, and while they might give answers that sound very convincing, they often get the facts wrong or make up things altogether. So it's up to you to make sure that you're being able to separate fact from fiction, because ChatGPT and other tools like these, they do make up a lot of data when you ask them questions. So you need to be able to understand what is real and what is not and how you can do further research to verify all of the claims.

BALAJI GOPALAN: At many schools, it's against the honor code to use tools like these for your assignments. If you're not sure, check with your student handbook, or ask your teacher if there are any ways that they would permit you to use AI for their class. And there are much better sources of information available online. For example, you could use Google Scholar to search for articles from academic journals. Those articles are reviewed by experts, so they're more likely to be factual. If you were writing a paper about cybersecurity, the National Cybersecurity Alliance's website would be a great resource.

KERI BARNETT-HOWELL: Depending on the situation, tools like ChatGPT could be very useful as a starting point. It can help with things like brainstorming or in the very, very early stages of research. For example, if you're asked to write a book report on any American novel published during the 19th century, you might ask ChatGPT to list some popular American authors from the 1800s so you can look them up yourself and see what book you might be interested in reading. But don't ask ChatGPT to write the essay for you. That's always a bad idea, and in college, it can and might get you expelled.

And it's also not going to write a very good essay. You, as a student, as a creative person, can write something much better than ChatGPT ever could. ChatGPT is a starting point. It is not your ending point.

There are automation tools out there specifically designed to detect the use of AI in essays and other school assignments, so it's better to steer clear. Instead, rely on your own knowledge, textbooks, and other resources provided by your teacher or that you can verify are legitimate.

WHAT'S ONE THING YOU WANT LISTENERS TO TAKE AWAY FROM THIS CONVERSATION?

LARRY KINKAID: That cybersecurity as a concept is not just limited to business. Again, because of the personal use cases of the internet and digital identities, it's everyone's responsibility, and there's some level of understanding and education that everyone needs to be aware of. And again, I think I mentioned it earlier, but you don't leave your laptop unlocked in a coffee shop. You don't leave your keys in your car. You don't leave things out that you wouldn't otherwise want to be taken. The same thing is true with digital identity. You don't want to leave your passwords reused. You also want to ensure that you're not giving it away through phishing emails. And you also want to ensure that your privacy is there. You don't want to broadcast to the world everything.

KERI BARNETT-HOWELL: Cybersecurity is everyone's responsibility. We all have a role to play in keeping our own data secure. That means we actively try to create secure passwords, we use password managers, and we don't write passwords down where they could be easily found by someone who shouldn't have them. There are simple steps that you can take today to improve your own cybersecurity posture.

LARRY KINKAID: I want them to take away that cybersecurity is ever-evolving. Best practices today—and I think, you know, again, passwords are best practice today, but in the short term or the long term, passwordless is right around the

horizon—there's always going to be something that we need to learn and implement, so it's something that you have to stay vigilant and constant with.

And again, especially as the internet becomes more and more part of our lives—we already saw the "Internet of Things" take over our homes. What's the next iteration of that? In my career, I've been doing this for about 10 years, and even before that on a personal level, the evolution of the cell phone, the evolution of social media, it's very different even over the past five years than it is today. So I think that's something to kind of keep in mind, that there's going to be more disruptors. There's going to be more education that comes along the way. But today, passwords, MFA, password managers—that is something that we are all responsible for and that's going to keep us secure.

BALAJI GOPALAN: The other thing to take away is the industry is constantly evolving and changing. Technology has come a long way over the last several decades. It's showing no signs of slowing down. By the time you're getting ready to start your career, there could be new jobs available that none of us can even imagine today. Keep your mind open, stay excited. You never know what opportunities might come your way.


BARR
ADVISORY