# Regions Insights Podcast

**Episode 1: The Dark Side of Digital Communication**

Cybercrime is a rising threat that knows few boundaries. In this episode, we'll explore phishing, smishing, and vishing — and explain how these schemes operate in plain sight and how you can protect what's most important to your well-being and finances. We'll hear from Regions cybersecurity specialists Jeff Taylor and Valerie Taylor, as well as tech veteran Kelly Jackson Higgins, Editor-in-Chief of the renowned cybersecurity news site "Dark Reading."

## *Episode Transcript*

**Chris Blose:** Welcome to The Regions Insights Podcast. I'm your host, Chris Blose, and on this show, we look at trends, tips and triumphs around your money.

If your work ever has you sitting at a computer or swiping on your phone, you already know about the power of digital communication. Our digital and social tools have unlocked a world of connections, both personal and professional, and processes to improve business.

But there's always a dark side. You've seen it in emails and text messages that looked legitimate until you check the details. You've heard it in urgent voicemails asking for your personal information. You've read about it in headlines about major data breaches.

With technology for the perpetrators and defenders of cybercrime developing at a rate faster than regulation, consumers and business owners need to stay smart about how they use digital tools. That's what our guests are here to help us with today. Later in the show, we'll hear from two members of the regions team — Jeff Taylor and Valerie Taylor — about identifying risks and what it means for your finances.

But first, we get context from Kelly Jackson Higgins, Editor-in-Chief of Dark Reading, an outlet that covers cybersecurity, and a longtime journalist with more than two decades covering the field.

**Chris Blose:**

So you've been working in the industry a while and you've witnessed the evolution of different types of cyber threats and different types of scams. Can you share some insights on the kind of

shifts you've seen and how these cyber criminals work and how cybersecurity has changed over that time that you've been covering the field?

**Kelly Jackson Higgins, Editor-in-Chief of "Dark Reading":**

Absolutely. So I've been covering security for probably about 25 years. But the early days of our coverage were things that seem kind of weird now and, and basic. One of the first, uh, big stories we had was the, the Veterans Administration. An employee took his laptop home with him and his house was robbed and laptop was stolen, and millions of veterans medical details and personal information was exposed. So there was this big move then to, you know, what do we do about these people moving their equipment around? Which seems silly now because literally everyone is mobile working. Back then some of the malware was pretty basic compared to what we see today. And it wasn't so simple to be a cyber criminal.

**Kelly Jackson Higgins:**

You had to have either a programmer writing malicious code for you or you know how to do it yourself. Whereas today, there's a whole cybercrime underground where there are specialists doing these things as a service, as a contractor. You don't even have to be technical to, you know, wage a ransomware attack. ~~A~~nd we had, you know, some more basic, I would say, breaches back then that were, that we look at today as that we don't see as much of. I'm thinking about back in the retail space, I guess it was around 2013,

**Kelly Jackson Higgins:**

They had a big payment card data breach. That was a big area that cyber criminals were focusing on was payment card data. Obviously you've seen since then how payment cards have are processed differently. You know, we have more checks and balances. Just because you get the number doesn't mean you can do much with it. So it really helped all their retailers, you know, sort of shore up their security, of their payment card systems. So they weren't exposed, the cards weren't exposed. It's always been about the money <laugh> that hasn't changed.

So the bad guys have now gone to back to the web-based approach. It really did sort of bring in this new wave of better security, but every time we had better security, the bad guys try to jump the bar and go like higher bar. So there's always this cat and mouse game of raising the bar for security. But yes, you're right, payment card information is still very valuable.

**Chris Blose:**

Right. So the approach is still somewhat the same, it's just maybe the target is a little bit different.

**Kelly Jackson Higgins:**

Exactly.

**Chris Blose:**

So I think you brought up something else interesting: the idea of somebody taking their work home and having a breach occur at home. You mentioned everyone's doing remote work in some form or fashion. Now we've got cloud services, we have all these other sort of different pieces of infrastructure and work style that we didn't have before. So how have those challenges, if you're trying to get in front of cybersecurity, how have those changed? How are people protecting their data and protecting their infrastructure at this point?

**Kelly Jackson Higgins:**

So there's kind of two things that happened. You know, there's more data out there now, right? That's stored. Everyone's digitalized, their, operations. And then you have workers working from home or the road or vacations, whatever. There's much more of that now. And then you also have more organizations going to the cloud for applications. So a problem that was always kind of systemic in the whole technology space was really knowing what was on your network. And back in the day when your network was in one location, it was still even hard, believe it or not, to know it was on it. And now you've got more pieces to your network that are movable or sometimes virtual. So trying to keep track of what's out there. And that could be your home user's mobile phone.

**Kelly Jackson Higgins:**

They're working off their home network where the kids are also on there. They have appliances who might, that might be connected to that network. At the pandemic, a lot of organizations, they did a lot more cloud-based applications to serve that user space and also to help secure things they couldn't see anymore. So the big challenge right now, and it's been exacerbated, is just figuring out what's connecting to your network. And until you see that you really can't fully secure your environment.

**Kelly Jackson Higgins:**

There's more tools out there, security tools. Um, there's something called zero trust, which is literally don't trust that thing, verify it no matter what it is. <laugh>, that's a really simple way to look at it. But it's sort of an approach that anything that connects your network assume right away is malicious and have these checks and balances to make sure that they're legitimate users using that connection, going through that connection. The whole IOT space is another problem, but it has gotten more complicated. The technology's gotten better, but there's still more, the biggest challenge I would say still today is knowing and always having a good visibility into what's connecting to your network.

**Chris Blose:**

So how can, and both individuals and then the organizations who are, you know, overseeing those individuals protect themselves from, you know, an attack on an appliance or an attack on

a smart device or, or something that it doesn't seem like it's part of the business environment, but may, by happenstance, become part of the business environment.

**Kelly Jackson Higgins:**

Yeah, so the tricky part is, you know, a business doesn't really have control over what you have in your house, right? So my company can't say, oh, Kelly, your stove is beaconing with its IP address, which actually happened <laugh> to me, like we bought a new stove and I had no idea I didn't buy a smart appliance on purpose, but apparently it has smart connection, which I was panicked when I saw that. You can't control that. So what you do is you add tools that sort of monitor the connections, whether that's a bpn, uh, cloud-based trust, zero trust, type service that every time that user logs in into your corporate network, there are these checks of balances that are making sure they have access only to what they need access to. You're checking their authentication with multiple factors, not just a password, but also like a second factor, to make sure they're who they say they are.

**Kelly Jackson Higgins:**

You know, obviously, one of the biggest tools and weapons for cyber attackers is to steal legitimate credentials. And we see that so often because it's so easy to steal them <laugh>, they're also being sold on the underground. So really making sure your users are coming in clean, and zero trust is one way to do that. Um, but they're also like other layers you can, you have like sort of monitoring, you have to constantly be assessing and reassessing your security architecture because it's a moving target now as your users are moving around, your devices are coming and going. The companies really can't just go in and, you know, police your local wireless network at your house. But what they can do is watch your, connect your connections into the corporate network and put some hurdles there to make sure it's legitimate traffic coming in.

**Chris Blose:**

So much of this space is seen as reactive and I think in the past it often has been. But some of these challenges that you're mentioning seems like they require proactive effort. So how can a company be more proactive as opposed to just reacting when an incident happens?

**Kelly Jackson Higgins:**

Yeah, I think I touched on some of that just sort of getting all these sort of, uh, I hate the term cybersecurity, hygiene or best, but it's really best practices having those in place. And it's really a constant, reassessment, right? Risk assessment. Getting a good view of what's on your network. Don't just wait for the breach to happen. Put things in place that can mitigate it. So if one user does get compromised, you can isolate them so it doesn't spread to the rest of the organization or their credentials aren't taken to get into more sensitive data in your environment. One thing that I feel like is underappreciated is the sort of the role of users. A lot of companies still kind of do the user training. It's this torturous, you sit through this video and you have to watch these dumb, you know, illustrations of, of users doing dumb bad things and

you feel as usually you feel kind of silly like you're in kindergarten doing this, this training, really bringing users on board is kind of part of the solution.

**Kelly Jackson Higgins:**

Making them feel like they're empowered to help your company and be part of the secure organization. I think that really helps when you make them feel like they have, a stake in it too. And not that they're the bad person if they accidentally click on something they're not supposed to click on. I think that really helps make the organization more secure. We've seen that a lot out there in our reporting. Also just having a really solid identity security strategy. And that means making sure that it's not just passwords that people are using to get into things, but there's multiple factors. And that of course you're patching all the security bugs that are sent, you know, the software that's sent out there. You can't patch everything, but basically be patching the high risk things in your organization. So I'd say a lot of it's risk assessment, constant, like not just one and done, you just have to keep doing it. It's an ongoing process.

**Chris Blose**:

And I'm curious too, what sort of trends are you seeing coming in the world of cybersecurity in the next few years? What sort of risks are we not thinking about yet, but we, we should be thinking about, for example?

**Kelly Jackson Higgins**:

AI to me is the most interesting thing because we haven't really, um, we're not really sure how it's gonna help, uh, attackers weaponize yet. But what's kind of interesting is that the security industry has really adopted it very quickly. Even though AI's been around a long time, I remember writing about it right outta college with an IT publication. I was working for IT before it was even a security issue. It's a concept and a technology, you know, it's evolved so much over the past few decades.

**Kelly Jackson Higgins:**

And of course chap GPT's release just accelerated it literally overnight. Like when that thing hit, it just, everything just was like wildfire with the AI discussion. Some of the security vendors right now are using it as a tool, uh, for things like vulnerability discovery. They're looking at ways to kind of help with their research. So it's kind of an arms race right now, I would say. I don't know how it's going to end. The good news is we have a little bit of a lead over the bad guys on it right now. But there's still a lot of things we don't know of how it could be abused, but that's probably the most interesting thing to me because it really did accelerate a lot of things. It accelerates almost everything. And there are some, there's some hype around it. Absolutely. I'm not trying to overhype it, but I think it's definitely something that we're keeping a close eye on and covering. I think it's shifting the mindset a lot on the defender side. The good

news is the defenders are ahead of the, of the attackers here in a way. That doesn't always happen.

**Chris Blose:**

<laugh>. Yeah. So this is a case with AI where not only is there a potential for criminals to use it, but defenders are actually using it to get ahead of the game in this case.

**Kelly Jackson Higgins:**

Yeah. And several security vendors have already announced AI, you know, based stuff in the past few months in the wake of chat G P T, like actually using a chat G P T type function in their security tools.

**Chris Blose:**

Yeah, if you had, you know, one bit of advice for someone who's running an organization and just wants to stay ahead of all of these threats and, and really be proactive in the future, what would it be?

**Kelly Jackson Higgins:**

I think one of the pieces of the puzzle, and we've been talking about this one for generations too, is authentication. How to make it not hard for your users, like make it where they don't even have to think about it. That's starting to happen a little bit with multifactor authentication. But if any of you help your relatives with their passwords, for example at home, and you see that their passwords are dog's name or whatever else, or their birthday, you know that it's still a huge problem, especially in the consumer space, which also spills over to the enterprise space. So I would say just getting on top of your identity authentication architecture is super important. Making everything multifactor.

**Kelly Jackson Higgins:**

If you look at your applications today at work, a lot of 'em aren't, they're just your password. So there really needs to be this really locked down of all applications that way and that way too, if those credentials are stolen and probably a lot of your credentials may well be in the dark web right now, for sale. If someone gets those, they can't just go use them to crack into your systems cuz they need that second factor to get in. So I think that's one of the ones that I think is super important.

**Chris Blose:**

Yeah. And that, that's one that can solve problems both for individuals and for ultimately the organizations as well.

**Kelly Jackson Higgins:**

Yes.

**Chris Blose:**
Yeah. Well thank you so much for joining us. We really appreciate your perspective and uh, thank you for the time.

**Kelly Jackson Higgins:**
Thank you Chris. It was great being here.

**Chris Blose:**
Now we'll hear from Jeff Taylor, Head of Fraud Forensics and Commercial Payments Strategy at Regions Bank. Jeff helps corporate and commercial customers when they become victims of fraud.

When Jeff joined us on the podcast in the past, he pointed out something important: The basic methods cyber attackers use don't change that much throughout the years. But their targets and the channels and techniques they use do. Criminals will always adapt their tactics to get past the security measures—which is where we started our conversation this time around.

**Jeff Taylor, Head of Fraud Forensics and Commercial Payments Strategy at Regions Bank:**
This is their job. This is what they do 24 hours a day and as their technologies change. The fraudsters are changing their approach to leverage new ways to appear legitimate and believable when the human element is involved. And humans are the line of defense in many of these cases, believability and trust are the most effective weapons and using social engineering, artificial intelligence, and technology enables the fraud attack to be much more believable]

**Chris Blose**: Jeff, what are some of the red flags that the communication you're receiving is not what it seems?

**Jeff Taylor:**
The first indication would be if the email text message or phone call comes from a sender that you don't recognize or from a party who would not normally communicate with you, like the company executive. I don't know about most of us. You know I don't get many emails or text messages from our CEO. If the email or text message expresses a sense of urgency or a demand that demands action immediately or secrecy between the parties, those kind of things are also red flags. if the call is important, the caller can always leave you a voicemail. if you recognize that those numbers are not something that you might receive a phone call from It's always a good practice to let them go to voicemail. And then lastly as I mentioned a moment ago

because of artificial intelligence, it's just not as good of an indicator as it has been in previous times so you have to be aware of poor senate structure punctuation and unusual wording in those email messages and text messages.

**Chris Blose:**
Yeah, something I've noticed too with the emails is I may get something that is from you know tech support at a certain company and they're using the branding of that company and they're using everything that looks like it's legitimate. But then you look at the URL or you look at the email structure and it's just a little bit off.

**Jeff Taylor:**
And that's exactly right and the the use of the new technologies to replicate and create very accurate communications from a language standpoint. Using artificial intelligence to be able to do that now makes that technique a little more difficult to recognize when the language itself has been artificially generated.

**Jeff Taylor:**
There was a case that was on national news media just a few weeks ago where a white hat Hacker created a deep fake audio or deep fake video of a well-known individual, a well-known reporter and sent that video to their to the person's assistant asking them to provide some personal information. When you watch that video and you look at that information, it's so believable and it appears to be what they've done is they've taken just pretty elementary software and be able to capture those videos and splice images together to create this deepfake video that looks and sounds like the person that you would have expected to be communicated with.

**Chris Blose:**
You know a lot of these tips that you're giving about red flags and things to watch out for. They're really going to be helpful for individuals. What about companies who are thinking about how to protect their information? And thinking about those employees who are either in the office maybe at home. You know, what sort of resources or training programs should they offer to make them less vulnerable to individual based attacks?

**Jeff Taylor:**
Well, there's certainly a number of different protective technologies available. So if you think about your mobile devices. There are ways to block calls from unknown callers, report and delete text messages. And software platforms to help protect devices from malware when a

new operating system's available. It's always a good idea to install it immediately as soon as you get that notification that that a new operating system is out there. We always suggest that businesses work with their information technology partners to ensure that their systems are up to date with the most current patches and software versions. Businesses should also leverage the protection products provided by their financial institution like positive pay with payee name Verification. And ACH positives to pay for unauthorized debits. Certainly encourage an employee education and awareness program for businesses, keeping your employees up to date on the latest fraud vectors is critical to their ability to recognize potential threats. And then thirdly developing that risk governance and response plan. You've got to know who you need to call and how to reach them because it's just like your business continuity plan, in the event of a natural disaster. If you had a natural disaster that forced your business to close then you've got

**Jeff Taylor:**
a continuity plan to help you come back up and running and get back up and running in order to service your customers. You need that same plan of action when you become a victim of fraud and that plan needs to also include your cyber insurance coverage and to the extent that you may have that coverage in your insurance policies.

**Jeff Taylor:**
A lot of our listeners are going to be interested in wealth planning and they may be high net worth individuals or high net worth families. Are there ever instances of targeting specific families or targeting specific people for their wealth and how do those risks differ in that case?

**Jeff Taylor:**
Oh sure. Ah criminals are typically path of least resistance people and so they're going to go where the money is and go where they believe the intended victim or potential victim is the most vulnerable. So if you think about high net worth families and individuals I think one helpful approach is to talk about the potential scams and discuss them with family members. Education and awareness are extremely important. Knowing what's going on and the types of attacks that are that are out there. High net worth individuals and families may have a more complex account structure that all the family members may not clearly understand. They also have greater resources that can make them a target. So it's just important that we have those kind of conversations both with our elder family members and younger family members those that are just becoming more adept and using their mobile devices and spending more time on those mobile devices because they're targets too.

**Chris Blose**:
Where can people look to learn about the latest threats?

**Jeff Taylor:**
Well believe it or not social media is a great place to do that. There are tons of resources that are available to both consumer and business segments. The Federal Trade Commission and the Consumer Financial Protection Bureau, both of those websites are great resources for individuals. And then businesses can utilize the sites that are hosted by the FBI, federal law enforcement, the cyber security and information security agency. It's called CISA. They're great resources, and then you can also obviously provide or and access the information that Regions provides on our Regions.com sites and the Region's Youtube channel.

**Chris Blose:**
I Know we often learn by looking at the cases where things went wrong as well. So are there any particular real-life examples or case studies that you can think of where you can really look at the methods that a criminal used and really learn from the consequences that an organization aced as a result.

**Jeff Taylor:**
I think it's important to note that these kind of malicious attacks are seen in every segment of business regardless of size or industry, and certainly consumers are under constant threat of scams. The two most common schemes that are experienced by business today are business email compromise and what we call or what the industry calls the trusted partner or imposter scam, and both of these can be intertwined to carry out the fraud. So in business email compromise the criminal will likely impersonate an executive, a vendor or an employee and request the creation of a payment or a change in the terms of an existing payment, so normally using email as a communications channel, the criminal would create a slight variation of the email address of the impersonated party and deliver the request. So it's very difficult to detect if you're not really paying attention. The content of the email might say something like, “We're changing our banking relationship...”

**Jeff Taylor:**
“…Please send your next payment to the new routing and account number provided below.” And so when you've got that kind of structure in the email that's instructing that person in accounts payable or payroll or someone who has the ability to originate a payment transaction. To make that change, in this particular case it might be 30 or sixty days before the actual payee contacts the company and reports that they didn't receive payment. Of course by that time the

money's long gone leaving you with an unpaid invoice and a financial loss in the trusted partner or imposter scam variation. The goal of the criminal may actually not be initially to or to get you to originate a payment but it may be their goal to obtain the victim's logging credentials. And then once they obtain those logging credentials they're actually able to create those fraudulent payments.

**Chris Blose:**
So paying attention to the little details, that's obviously one sound bit of advice. Is there any other advice that you typically give people on trying to stay on top of this?

**Jeff Taylor:**
Yeah, absolutely the one approach to helping prevent this attack is to establish internal controls before the payment's actually being made, that's applicable not only in the business segments but also in the consumer segment. So one of those is called dual control, and it's when you have a secondary approval where an additional signoff is required before a payment's released. The one I think that gains the most traction from a business email compromise standpoints a is a control that we call stop, call and confirm. If you receive a message like this, you stop your process, pick up the phone and call the requester at a number that you know.

**Jeff Taylor:**
Don't call the number in the email or respond to the number or respond to the email because that's likely going to be the criminal that you're going to be communicating with. You want to call them at a number that you know and then confirm with them that that request is legitimate. I just know it's a quick phone call that can potentially save you a lot of grief.

**Chris Blose:**
“Stop, call and confirm” feels a bit like the old “stop, drop and roll” advice many of us received as schoolkids, and it’ll help put out a different kind of fire. Jeff Taylor says it’s a part of creating a culture of fraud awareness, which is a really critical step for individuals, families, and businesses.

Part of that awareness is just knowing in broad strokes the kind of attacks that happen. There’s phishing, the email-based attacks that have been happening for decades. There’s spear-fishing, the more targeted version of that that goes after high-level decisionmakers and high-worth individuals. There’s smishing, which comes across via SMS text messaging. And increasingly there’s vishing, which comes via voicemail.

To learn even more about the risks we need to watch for, we have Valerie Taylor joining us. She's the Senior Vice Preisdent of IT Risk Management and Non-Financial Risk Management at Regions Bank. Valerie echoed her colleague's warnings about business email compromise and talked about a preventative technique that can help prevent it: employee education.

**Valerie Taylor, SVP of IT Risk Management and Non-Financial Risk Management at Regions Bank:**

I do think employee education is very important. I think it's important to keep these types of examples kind of in the forefront of people's minds, especially employees who might be targeted finance departments, HR, you know, people who have access to lots of data or have the authority to make or change payment details. What I have seen or heard from colleagues, you know, throughout the industry and in other industries, that has worked, is this continuous training. So you might do some simulated phishing of your own employees where you send an email that is crafted to look like what would come from an attacker or a scammer. And what you're looking for is for your employees to be able to identify that email and report it. So you need to have a good reporting chain as well and make it easy, right? Put a button right there in the mail client so that someone can say, I think this is a phishing attempt.

**Valerie Taylor:**

And then you also respond back to say, "Congratulations, you spotted this month or this quarter's fishing attempt." Another thing that I've heard that works well, Chris, is to incentivize this type of behavior. And so I've seen some programs that instead of punishing people who might not pass those simulated exercises, they give you a reward if you do pass. You might get a gift card from your company that says, "Hey, you passed our last fishing simulation. Thank you for being part of the solution."

**Chris Blose**:

What about the technical side of things? What has changed in the world of technical solutions or infrastructure that companies can put in place to protect themselves from fraud?

**Valerie Taylor**:

So I think there are a lot of options, especially when you're talking about phishing or vishing or smishing now as well, which is, you know, you have your email, your voicemail and your SMS: phishing. You have solutions in place where you can do filtering of those messages. Most, I would say companies are doing email filtering. And so what you're doing there is you're stopping the message from even getting to the employee. Obviously as far as, uh, solutions go, you wanna prevent as much as you can. Then there's detective solutions as well. So that's more gonna be, maybe your web filtering too. So let's say the message does get through to the employee, they click something, you can block those outgoing connections, right, if they look suspicious to your tools. You can also implement, you know, multifactor authentication. And

that might help because, what tends to happen with phishing is it's a way for an attacker to get a foothold into your organization and potentially to have your associate or your employee provide their credentials and then those credentials get compromised. But if you have another layer of authentication, that might make those credentials not as useful.

**Chris Blose**:

Yeah, have if people in increasingly pushed for that multifactor authentication? Cuz I know even just among individual users, that it may not be that widespread when you think about all the different places you have to log in.

**Valerie Taylor**:

Yes. So definitely I think in the corporate level, especially for banks, you will see that multi-factor authentication. I think one thing that I've heard people talk about though is this notion of MFA fatigue where you are getting so many prompts to re-authenticate that sometimes you're not paying attention. And I think that is an important part of training and the conversation is to let people know you need to really make sure that you initiated this login attempt and that you're not just blindly accepting the MFA push.

**Chris Blose**:

Yeah. It's so easy to ignore a security alert or something in email if you get a million of them <laugh>.

**Valerie Taylor**:

Yes, it is.

**Chris Blose**:

Yeah. I'm curious too, you know, we're talking of a lot about proactive approaches, which I think is, is how companies probably should address this, but what about the reaction as well, right? If a company has had a successful phishing, vishing, smishing, whatever the next ING is, attack, what steps should they take to minimize the effect of that and to recover quickly and then possibly put some measures in place to prevent that in the future?

**Valerie Taylor**:

I think what's really important there has to happen before the event takes place. And that's having a really good incident response plan in place and having your business continuity plan in place, not just in place, but that you've tested the plans and you know that they're going to work. Because once an incident starts, then you need to be able to rely on that plan to effectively mitigate what's happening. You know, isolate whatever devices or parts of your network you need to isolate, work on the mitigation there, and then restore services and data if you need to. And that all comes from having a solid plan that's tested and that you can execute.

**Chris Blose**:

Yeah. One thing that strikes me too is that at this point we're dealing with a lot of, a lot more channels than maybe companies or even individuals we're thinking about 10, 15 years ago. You've got messaging apps, social media platforms, other digital communication channels. We're all on video chat now, you know, which we weren't necessarily a few years ago. How does that world of different platforms and different channels affect the way you have to approach, prevention of cyber crime?

**Valerie Taylor**:

So I think there, what's important is that you only give kind of the level of access that's required. So across those channels, like if you have, let's say a marketing function that needs to have access to a Twitter account in order to communicate with customers, maybe you make sure that, those individuals can't reach other parts of your network. So you can isolate as much as possible, but I think that education is key here as well, because you are moving across channels, people do need to be pretty vigilant in how they interact with those different channels.

**Chris Blose**:

Now for somebody who's interested in staying on top of what the latest sort of forms of attacks are or the latest trends in this space, so that they can be ahead of it, how would you recommend that they follow information about this?

**Valerie Taylor**:

Um, do you mean from a defender standpoint or a layperson, or what do you mean?

**Chris Blose:**

Let's start with the defender's standpoint.

**Valerie Taylor**:

So I think, you know, there, there are so many options there for staying up to date. I personally just subscribe to a variety of different newsletters. So I get different news in my inbox daily and then I kind of follow those threads. Lots of people set up lists on Twitter, based on certain keywords and that will bring them, you know, the latest information. I like Reddit, personally. So the information is out there, it just depends on what your specialty is, and what it is that you're interested in. You can look for news to be delivered to you and then you can also set up different keyword searches to bring you items that would be relevant to you.

**Chris Blose**:

And then I think just for the average individual or user too, like, what should they really be concerned about how they stay, on top of this?

**Valerie Taylor**:

So I think what you'll hear, ua lot of the advice for, you know, the person at home or individual users is not to reuse your passwords, you know, and it's hard, right? Because we have a password for everything. And so it gets pretty difficult to remember and to choose strong passwords. So in those cases, I would say make use of a password manager and make sure that your password manager is generating strong passwords for you. Use a multi-factor or two-factor authentication option if it's available to you where you're logging in as well.

**Chris Blose**:

Yeah, it seems like not skimping on the multifactor is is is pretty important these days, even if we all have a little fatigue from it.

**Valerie Taylor**:

Yes.

**Chris Blose**:

Yeah. Well, thank you so much Valerie. We really appreciate your time and your perspective today.

**Valerie Taylor**:

Thank you.

**Chris Blose**: If there's one key takeaway from today's guests, it's to pay attention to the details. Check the email address on that suspicious message closely. Use multi-factor authentication even if it takes a little extra time and attention. Stop, call and confirm.

Thank you to our guests Kelly Jackson Higgins, Jeff Taylor and Valerie Taylor for this sound advice. And thank you for listening. You can check out future episodes and more info at URL TK.

*they threat evolves daily. There's no guarantee that all fraudulent transactions will be prevented or that related financial losses will not occur. Visit Regions.com/stopfraud or speak with your banker for further information on how you can prevent fraud.*