Bank of Botetourt

November 2022

Cybersecurity Awareness Month 2022

#See Yourself in Cyber

Cybersecurity Awareness Month – observed every October – was created as a collaborative effort between government and industry to ensure every American has the resources they need to stay safer and more secure online.

Since its original inception under leadership from the U.S. Department of Homeland Security and the National Cybersecurity Alliance, Cybersecurity Awareness Month has grown exponentially, reaching consumers, small and medium-sized businesses, corporations, educational institutions and young people across the nation. Now in its 18th year, Cybersecurity Awareness Month continues to build momentum and impact co-led by the National Cybersecurity Alliance and the Cybersecurity and Infrastructure Agency (CISA).

See Yourself in Cyber

This year's Cybersecurity Awareness Month's campaign theme was "See Yourself in Cyber" and represents that cybersecurity is ultimately about people, which means seeing yourself in cyber no matter your role.

According to the Cybersecurity and Infrastructure Security Agency's (CISA) website, "this year's campaign theme demonstrates that while cybersecurity may seem like a complex subject, ultimately, it's really all about people." Through this campaign, the CISA highlighted the key actions people should take, including enabling multi-factor authentication, using strong passwords, recognizing and reporting phishing, and keeping your software up to date.

Technology can only do so much; it's people who remain our greatest strength.

Security Starts with Awareness

In today's boundaryless workplace, comprehensive security is essential. That kind of 360-degree protection requires education and awareness to safeguard identities, data, and devices. Awareness programs help enable security teams to effectively manage their human risk by changing how people think about cybersecurity and helping them practice secure behaviors. The SANS 2022 Security Awareness Report analyzed data from more than a thousand security professionals from around the world to identify how organizations are managing their human risk. The report found that more than 69 percent of

Connect with us!

(540) 591-5000

Continued on Page 2

security awareness professionals are part-time, meaning that they spend less than half their time on security awareness.

According to the SANS report, cybersecurity awareness professionals should endeavor to:

- Engage leadership by focusing on terms that resonate with them and demonstrate support for their strategic priorities. “Don’t talk about what you are doing, talk about why you are doing it.”
- Consider having a 10-to-1 ratio of technical security professionals to human-focused security professionals.
- Partner with other departments in the organization—such as communications, human resources, and business operations—to help engage and communicate with your workforce.
- Make the training simple to understand and follow. “Just like working out—it’s the frequency that’s important.” And dedicate time to collecting information about the impact of your awareness programs.

It’s Up to Each of Us to #BeCyberSmart

In 2022, the most common causes of cyberattacks are still malware (22 percent) and phishing (20 percent).4 Even with the rise of ransomware as a service (RaaS) and other sophisticated tools, human beings remain the most reliable, low-cost attack vector for cybercriminals worldwide. For that reason, it’s vital that we all stay informed about how to prevent breaches and defend ourselves, both at work and at home.

Here are some basic steps we can all take to #BeCyberSmart:

Phishing: Deceptive emails, phony websites, fake text messages—these kinds of phishing scams accounted for 30 percent of attacks in 2021.

- Check the sender’s email address for verifiable contact information. Common phishing tip-offs include a misspelled or unrelated sender address. If in doubt, do not reply. Instead, create a new email to respond.
- Don’t click on links or open email attachments unless you have verified the sender.

Devices and software: Unpatched, out-of-date devices and software are a leading access point for cybercriminals. That’s why practicing good cyber hygiene is so important for avoiding destructive malware that can steal users’ personal information. To help keep your devices safe:

- Enable the lock feature on all your mobile devices.
- Activate multifactor authentication on your sensitive apps and accounts.
- Run antivirus software and install system updates immediately.

Scams: Criminals will often contact you seeking to “fix” a nonexistent problem. The email or text message will contain a sense of urgency, such as “Act now to avoid having your account locked!” If you see this type of message, do not click the link. And remember to always report any suspected scam so the organization can take action. A few tips to remember:

- Be skeptical of unsolicited tech support calls or error messages requesting urgent action.
- Do not follow any prompts to download software from any third-party website.
- When in doubt, open a separate browser page and go directly to the company’s webpage.

Passwords: Passwords are our first line of defense against unauthorized access to accounts, devices, and files. However, the average person now has more than 150 online accounts; password fatigue is always a danger. Some tips on how to protect your passwords include:

- Use your browser’s password generator to create stronger passwords.
- Avoid accessing personal and financial data using a public wireless network.
- Use a password manager, or consider going passwordless.

Cybersecurity Awareness Month is a special time for us as we collectively come together—industry, academia, and government—to promote the importance of a secure online environment. We know that cybercriminals are persistent and driven, working all day, every day with no days off. That’s why we need to work together on awareness and education year-round and build a culture of cyber defenders. Everyone has a role to play in cybersecurity, and when we learn together, we are more secure together.

Source: *National Cybersecurity Alliance*
Source: *Microsoft Security*

Starting at Home: Cybersecurity in the Hybrid Workplace

As people settle into the late stages of the pandemic, the hybrid workplace is not going anywhere. Therefore, the enterprise must address the increasing number of entry points into the network as more employees work remotely.

In 2021, 61% of malware directed at organizations targeted remote employees via cloud apps. Since the onset of the pandemic, about 30% of organizations have reported a spike in cyber attack attempts.

It's been harder lately to manage the logistics of where employees connect. So, it's no wonder that 54% of IT workers are on edge about the possibility of future cyber attacks.

However, people often don't understand the hybrid work model. The only way the enterprise can address the myriad challenges is to gain a solid grasp on how the workplace is really evolving.

What Is the Hybrid Work Model?
The hybrid model combines a remote and a regular on-premise workforce. Employees want to be flexible in where and when they work. Plus, as new tech constantly develops, the workforce is becoming more virtual.

This modern work model is not one-size-fits-all, and each company's version will be unique. The most successful hybrid solutions are flexible and agile, so they can meet the ever-changing demands of management, employees and any regulations.

According to an Economist Impact survey commissioned by Google Workplace, more than three-quarters (75%) of employees and managers expected to adopt the hybrid work model within their business or agency in the next three years.

Cybersecurity challenges in adopting the hybrid work model fall into three basic categories: data, devices and behavior.

So Much Data
Whether employees are hybrid, remote or work in the office, they have access to an increasing amount of sensitive data. The business must safeguard that data. As the attack surface widens, data protection becomes more difficult.

But data protection has always been critical, and while hybrid makes the issue worse, it's the skyrocketing number of devices and endpoints that stand out.

All These Devices
The ever-growing number of other devices in our lives presents significant obstacles for enterprise security in a hybrid work environment. Employees returning to the office are doing so with not just one device but a steady wave of new ones. Many questions arise from this:

- Did the organization issue their devices?
- Does someone regularly update the OS or firmware?
- Are all software patches in place?
- Do you know all of the networks the device has connected to? What other parties have been on those networks?

User Behavior
According to IBM's 2021 Data Breach Report, the average cost of a data breach due to remote work was $1.07 million higher in those attacks in which remote work was a factor. While lack of the right technology or resources certainly plays a role, online employee behavior is a critical cause.

As we adapt to the ever-changing shifts in society, humans are not at our best. The adage still applies: humans are the weakest link in the cybersecurity chain. Thinking about threat actors is not top of mind for many employees as they tackle their daily tasks. The threat actors are well aware of that.

Hybrid Work Model Strategies
As always, the best strategies start with the basics. Good security hygiene applied as much before the pandemic as it does today. What this means is you'll want to ensure:

- Remote employees use a VPN
- Employees know cyber attacks could happen
- Employees can access only the resources they need
- Your team patches systems often
- Your networks are segmented.

When it comes to network segmentation, it's important not to limit this to the corporate network. Employees working from home should consider splitting their home network into work and home segments. Most internet providers today can accommodate this setting. Especially as more internet of things (IoT) devices are brought into the home, the potential damage of an attack increases. With segmentation, if an attacker hits an IoT device because of the actions of another family member, the payload won't wreak havoc on other network devices.

Whether or not you decide to include home network segments, you need to back up your strategy with some sort of robust policy. Update those policies to address the hybrid work model. From the C-suite to all employees, make sure everyone is aware of the policies and adheres to them. Monitoring services and tools like identity and access management are critical here.

For employees working from the office, you'll need to decide how you're going to treat all these new devices — whether bring-your-own-device or corporate-issued. Do you expect employees to follow certain rules before returning to the office? Do you have a clear understanding of what constitutes a trusted device? You should be aware of not just what actions you can take but how you'll respond if a security threat occurs.

The Meeting of Zero Trust and Hybrid Work
But perhaps the most efficient way to address the security challenges is adopting a zero trust strategy. With a blueprinted zero trust approach, organizations can empower their workforce by correlating security information across all domains and quickly grant conditional access based on the model of least privilege.

Finally, your team will need to be transparent about their policies, rules and standards. The more transparent you are, the less likely it is employees will perceive your team as the enemy.

Source:* *Mark Stone, SecurityIntelligence