Cybersecurity for Businesses

7 Ways to Stay Safe

Avilar Technologies, Inc. | 6760 Alexander Bell Drive, Suite 105 | Columbia, MD 21046 | (888) 759-7053 | www.avilar.com

Massive data breaches. Crippling ransomware attacks. Diversions of sensitive information to malicious hackers. Faced with these headline stories, many of us feel powerless to stop cyber attacks. We're inclined to defer that responsibility to cybersecurity professionals whose job it is to monitor and respond to cyber threats and incidents. Yet, the truth of cyber resilience is that each of us has a part to play.

Since 2004, October has been designated Cybersecurity Awareness Month – a time for government, corporations, and nonprofits to help raise cybersecurity awareness across the country and around the world. Here are seven ways to keep your company cyber-safe this National Cybersecurity Month.

NUMBER ONE: Educate Your Workforce

This year's campaign theme is "See Yourself in Cyber." It's meant to demonstrate that, while cybersecurity can seem daunting or complex, it really comes down to individuals. Everyone is encouraged to make smart online decisions – whether at home, at work, at school, or in the community – today and every day.

Unlike previous years, which had weekly themes, the 2022 campaign features four key behaviors to combat cyber attacks (#2 – #5, below). This month, encourage all employees to practice these cyber-smart behaviors. Remind your employees, contractors, managers, and leadership team about their role in keeping your company cyber-secure.

To point them in the right direction, send an email promoting National Cybersecurity Awareness Month activities, tips, and resources. Include relevant articles in your company newsletter. Share cybersecurity tip sheets. Promote your basic cybersecurity learning opportunities for your full employee lifecycle.

Some companies are planning events to engage employees. Cyber-related "fairs" with a mix of education and fun cyber-themed events may work at your company. Try online games with prizes for individuals and teams who get the most correct answers or fastest response times. Or participate in any of the National Cybersecurity Alliance (NCA) online events for the public, including an expert presentation, a #CyberChat Twitter Chat event, and an Afterglow Party.

NUMBER TWO: Think Before You Click

In a phishing attack, the perpetrator sends a message – a text or email – designed to lure someone to disclose login credentials. The perpetrator pretends to be a trusted organization or known contact and urges

action – usually clicking on a link. When unsuspecting victims submit their login information, the cyber attackers collect the information and use it to gain access to real websites and systems. A phishing attack can cause extensive financial harm to individuals and companies.

These days, phishing attacks are quite sophisticated and can be difficult to detect. If an email, text message, or link looks or seems a little off, don't click. It could be an attempt to get sensitive information or install malware.

In your emails and newsletters, let employees and contractors know what to do – and who to contact – if they receive a questionable message.

NUMBER THREE: Update Your Software

This is the second key behavior urged by organizers – and an important one for employers, whether their employees are using company-supplied laptops and phones or their own devices.

Throughout the month – and all year long – remind employees to act quickly if they see a software update notification. Often, updates contain changes that address security vulnerabilities, so the sooner people start using the newest version, the more secure their (and your) systems will be.

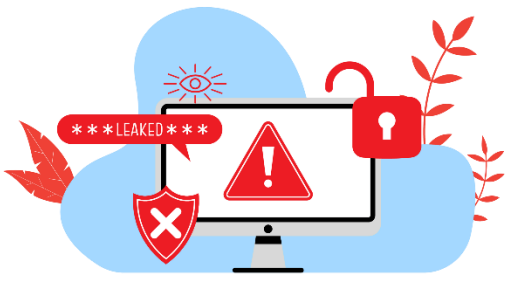
It's easiest – and safest – to turn on automatic updates. Check with your leadership and IT teams to see whether you can require automatic updates at your company.

NUMBER FOUR: Use Strong Passwords

So many of today's websites require user accounts to access the content or services they offer, insisting that users create a password. The problem? As PC Magazine points out, "Some people get the bright idea of using the simplest possible password, like '123456789' or 'password.' Others memorize one superbly random password and use it for everything. Either strategy is likely to make you the latest victim of identity theft."

A "strong" password is one that is long, unique, and randomly generated. Using strong passwords has become easier in recent years, with the emergence of random password generators and password managers. A password manager will generate and remember different, complex passwords for each individual account, encrypting them and keeping them more secure.

Some small companies will subscribe to a password manager for their employees' work-related passwords. Others will encourage or require employees to use one for all their passwords.



NUMBER FIVE: Enable Multi-Factor Authentification

Enabling multi-factor authentication, or MFA, is one of the most effective steps your employees can take to reduce the chances of getting hacked. It's also the one they're most likely to resist.

MFA, also known as "two factor authentication" or "two step authentication" is a layered approach to securing data and applications where the system requires users to present two or more credentials before logging in. A password plus the answer to a security question. Or a fingerprint with a one-time security key.

Many employees resist setting up MFA because of the "hassle factor" or having to remember or look up the second credential. Try sharing this 90-second video from the Cybersecurity and Infrastructure Security Agency (CISA), which emphasizes that "implementing MFA can make you 99% less likely to get hacked" and shows how easy it is to turn on MFA.

NUMBER SIX: Build and Strengthen Your Cyber Workforce

Another "angle" of the "See Yourself in Cyber" theme speaks to cyber professionals and those aspiring to join the cyber workforce. CISA and the NCA are talking to business and community leaders across the country about how to build a bigger, more diverse cybersecurity workforce.

To recruit a diverse cybersecurity workforce, be sure you're hiring for skills. Take a competency-based approach to performance management, to ensure your cyber workforce is building the skills they need and getting the opportunities and promotions they deserve.

October may be a good month for you to "check in" with your cybersecurity personnel. Conduct skills assessments to see if they are keeping their skills current. Check to see if their certifications, too, are up to date. Also remember to see if they're getting what they need from your organization. Do they have the tools, the support, the opportunities they're looking for? This "check in" may be one way to ensure that these employees are engaged (not Quiet Quitting) – and motivated to keep your company secure.

NUMBER SEVEN: Update Your Business Continuity Plans for Cyber Resilience

If you haven't already, update your business continuity plan to incorporate cyber threats and attacks. Review plans and protocols with your team, including assigning responsibility to track industry

developments and incorporate best practices.

As one example, following several high-profile ransomware attacks, CISA and the Multi-State Information Sharing and Analysis Center developed a Ransomware Guide with a detailed checklist for what to do when a ransomware attack occurs. It's a tricky situation. The FBI and other law enforcement strongly urge against paying ransom to cyber attackers, who may be energized by the result and motivated to do more harm. However, a ransom payment may be less expensive than the cost and personnel required to restore or rebuild systems. Encourage your business continuity team to work through tabletop exercises and healthy debates to come up with a plan and protocols – before an attack forces difficult decision-making under duress.

In Conclusion

We live in an increasingly digitally connected world where cyber attacks are becoming more widespread and sophisticated every day. Companies, regardless of size or industry, must take proactive measures to combat the growing threat. And the most effective actions require every employee to do their part.

Is your team focused on building a cyber-resilient organization? Contact us to find out how a competency-based approach can help. Then schedule a demo to see how Avilar's WebMentor Skills™ competency management system can support your efforts.

About Avilar

Avilar – The Competency Company™ is a leader in workforce development and planning with web-based competency management and learning solutions for corporations, government, and non-profit organizations. In 1997, Avilar pioneered its award-winning WebMentor™ product line and has built itself on the basis of superior customer service and highly adaptable product design.

Avilar consultants are recognized as industry thought leaders and have decades of experience in implementation and analysis. Let Avilar help you transform your organization from ordinary to extraordinary.