Responsive Technology Partners

Issue 51 | April 2023

DON'T BE THE FOOL

That Gets Caught in Cyber Showers

April Fools can be a time for cyber criminals to trick people into falling for their schemes. Don't be fooled this April by having good cyber hygiene and be wary of these threats.

"The National Security Agency reports that 93% of all attacks could be stopped with basic cyber hygiene practices." (XM Cyber).

Having good cyber hygiene requires background knowledge and awareness of cyber trends amongst threat actors. Some tactics to be aware of this April Fool's Day include phishing scams, deepfakes, and ransomware and malware.

Phishing schemes typically include malicious links that download malware when clicked on. Malware is malicious software.

Ransomware is a specific type of malware that holds your data for ransom. Ransomware is an obvious choice for cyber-attack when wanting to pull a prank, such as an April Fool's Day prank.

To avoid these schemes, improve cyber hygiene by being familiar with phishing scheme tactics and incident response plans for if a breach were to occur. This will leave your company more prepared preceding and following a cyber-attack.

"In the modern age, cyber criminals also play "pranks" on unsuspecting users and organizations. Just as attackers have taken advantage of every holiday, pandemic, or political situation to capitalize on user naivety, fear, or love, they are certainly prepared to exploit April Fools. Back in 2009, the Conficker C computer worm was programmed to stay dormant until April 1." (Sangfor).

Deepfakes are another popular way threat actors "prank" citizens and businesses. Deepfakes utilize artificial intelligence to produce realistic audio and visual content that is completely fabricated. It is often used to paint someone in a bad light in video or audio form. It can also be used to spoof phone calls, opening another security threat entirely where threat actors can obtain financial information directly from you.

Cyber hygiene is the solution to all of these issues. With good cyber hygiene, cyber-attacks are less likely to occur due to human error, and a majority of cyber-attacks can be prevented with good cyber hygiene.

UNDERSTANDING CYBER SECURITY COMPLIANCY STANDARDS

There is an endless number of things a business owner should do for their business to be successful. They must develop a product or service that can attract customers, hire and train a team to oversee day-to-day operations, implement marketing strategies and so much more. While all these tasks are essential for your business to be profitable, your business will never get off the ground if you aren't compliant with standards that affect your industry.

Compliance standards are guidelines or rules that organizations must follow to meet legal, regulatory or industry requirements. These standards are designed to ensure organizations ethically conduct business – by protecting the rights and interests of their customers, employees, and other stakeholders. When an organization does not maintain its compliance standards, it will be met with fines, legal action, and other penalties.

National Institute Of Standards And Technology (NIST)

The NIST is a nonregulatory agency of the United States Department of Commerce that promotes innovation and industrial competitiveness. As a business leader, you must be aware of the various cyber security standards and guidelines set by the NIST. One such standard is the NIST Cyber Security Framework, a voluntary framework that provides a way for organizations to better manage and reduce cyber security risks. It's built on the following five core functions:

Identify

It's vital to understand the organization's cyber security risks, assets and the people responsible for them.

Detect

It's important to detect when a security incident occurs. This function includes activities like monitoring network traffic and reviewing logs.

Recover

After a security incident does occur, organizations must know how to restore normal operations as well as their systems and data. This process often helps people understand the importance of implementing safeguards to ensure similar incidents do not occur in the future.

Protect

Implementing the necessary safeguards to protect the organization's assets from cyberthreats can shield companies from increasing risks.

Respond

By responding to security incidents as they occur and containing the incidents, people can eradicate the threat and recover from it.

Health Insurance Portability And Accountability Act (HIPAA)

The compliance standards set by HIPAA are some of the most well-known as they pertain to protecting personal health information (PHI) in the United States. HIPAA requires covered entities, such as health care providers and health plans, to ensure the privacy and security of PHI. The Security Rule and the Privacy Rule are the two main sets of regulations under HIPAA that covered entities and their business associates must follow.

The Security Rule sets standards for protecting the confidentiality, integrity and availability of electronic PHI and requires covered entities and business associates to implement certain administrative, physical and technical safeguards. On the other hand, the Privacy Rule sets standards for the use and disclosure of PHI and gives individuals certain rights concerning their PHI – such as the right to access their PHI and the right to request their PHI be amended.

Failure to comply with HIPAA can lead to significant financial penalties, reputational damage and, in some cases, the loss of a license to practice medicine.

Cybersecurity Maturity Model Certification (CMMC)

The CMMC is a relatively new set of compliance standards developed by the Department of Defense to protect Controlled Unclassified Information. The CMMC is mandatory for all DoD contractors and subcontractors that handle CUI. This is a tiered certification system with five levels of maturity. Each level has a specific set of practices and processes that organizations must implement to achieve certification. As a business leader, you should be aware of the CMMC and the specific level your organization will need to achieve to comply with the DoD contract requirement. CMMC certification is audited and managed by a third party. Keep in mind that getting this certification will take ample time and effort. You'll need to implement robust security protocols and practices that may not have been in place before.

These are just a few compliance standards that may be required in your industry. Complying with these standards will help protect your business, customers, and employees.

LET YOUR EMPLOYEES KNOW YOU CARE WITH THESE 3 TACTICS

If an employee is unhappy working for your company or doesn't feel appreciated by their leadership team, they will search for a new job. This has left many leaders questioning what they can do to show their employees they actually care about them and their well-being. Here are a few different ways to show your team you care.

Growth Opportunities

Most employees want to work somewhere with the potential for advancement. It's important to connect with your employees through one-on-one meetings so you can determine how they want to grow professionally and personally.

Foster A Supportive Work Environment

Nobody wants to work at a business where they don't feel accepted, supported or appreciated. Go out of your way to create an inclusive environment and give your team a sense of belonging.

Recognition

Your employees want to hear about it when they do well. Don't be afraid to recognize or reward them when they're doing a great job. Simply thanking your employees for their hard work can go a long way toward improving overall morale.

ARE YOU MICROMANAGING YOUR TEAM?

There are many different management styles, but one that always seems to upset employees and take away from productivity is the act of micromanaging or overcoaching. Micromanaging occurs when a leader provides instructions that are too specific while watching over the team as they perform their tasks, looking for any lapse in perfection they can then bring up to the employee. It's a frustrating practice that can send well-qualified employees running out your doors.

So, how do you know if you're micromanaging your team? Pay attention to how you're directing them. You won't get a preferred response if you tell your billing manager how to do their job. You hired these employees to perform specific roles, and they have the experience to do it well. So, let them work until there's a need to redirect or re-analyze the situation. Ask for feedback when you conduct one-on-one meetings with your team. Listen and make the necessary adjustments if they say you're micromanaging. This will help boost productivity in your business while you still get the most from your team.