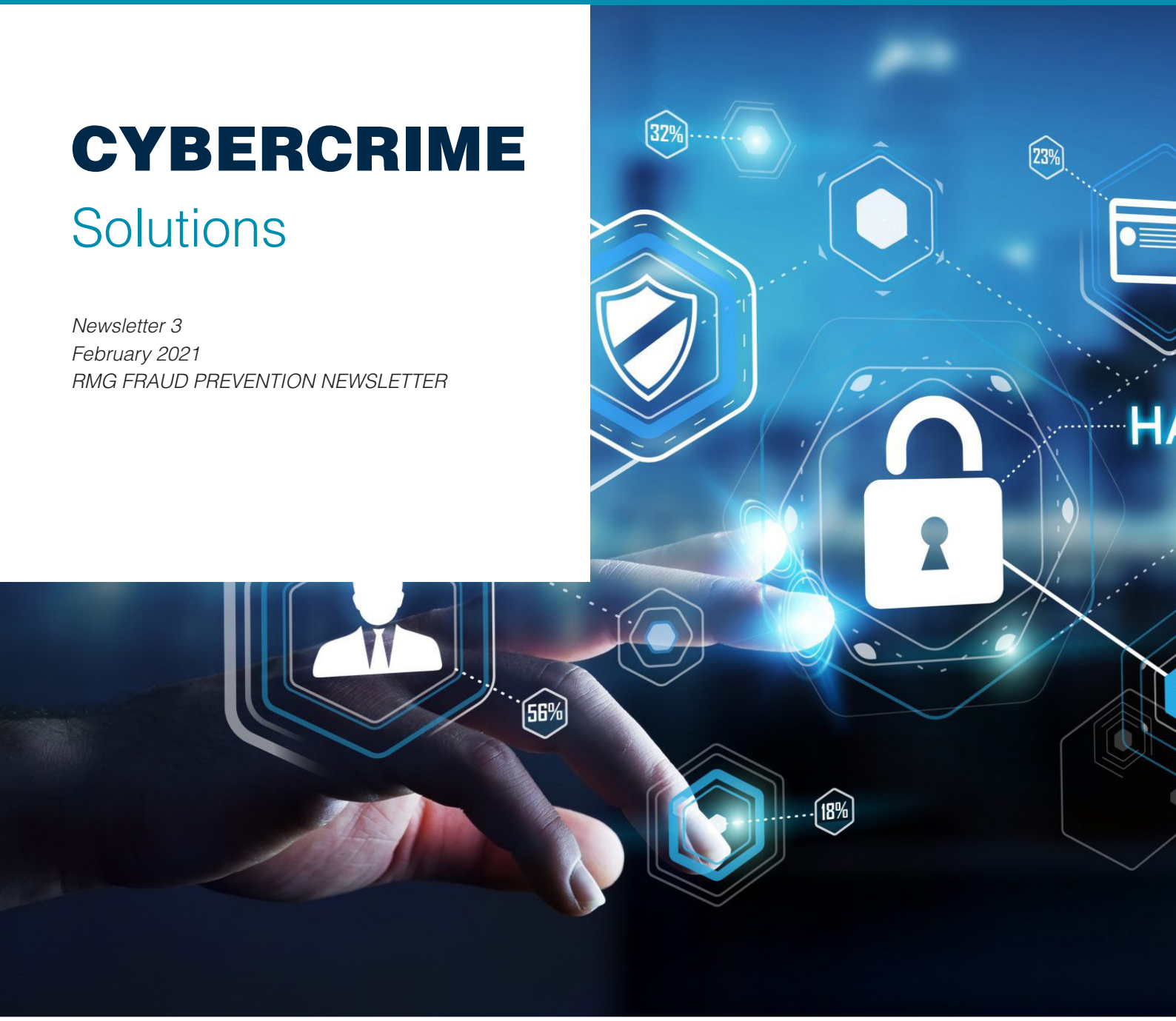
CYBERCRIME

Solutions

Newsletter 3
February 2021
RMG FRAUD PREVENTION NEWSLETTER



www.rmgforensics.com

INSTITUTE OF DIRECTORS SOUTHERN AFRICA

UNASHAMEDLYETHICAL

RMG
FORENSIC SERVICES (Pty) Ltd.

Contents

1. Keep all software updated and regularly patched....2
2. Invest in a reliable VPN....2
3. Educate and train your staff....2
4. Divide, encrypt, and back up sensitive data....3
5. Set up strict limitations on company computers....3
6. Use anti-virus software and keep it updated....4
7. Use strong passwords....4
8. Two-factor authentication....5
9. Follow industry best practices and guidelines....5
10. Implement email security solutions and phishing simulations....7

Foreword

As part of the Fraud Awareness initiative of the MRG Group to its members this monthly Fraud newsletter would assist with the most current Fraud Trends detected in the industry as well as practical advice to proactively remedy this.

In this month's fraud newsletter version 3/ 2021 we cover the subject at hand: cyber crime solutions. We will explain the definition and these modes operandi of the fraud and provide tips on how to prevent it.

In the next edition newsletter version 4 / 2021 in the first quarter of the year we will define cyber security threats in the South African and in the global context.

These days, businesses have less reason to fear burglars and thugs than anonymous cybercriminals. While thieves can steal merchandise or damage property, cybercriminals are much more insidious, and the harm they cause can be orders of magnitude worse. When sensitive information is stolen or financial accounts are hacked, the losses can overwhelm even the most spectacular robbery.
It is not only large global corporations that are targeted; cybercriminals often go after lower-hanging fruit. Smaller businesses are often less likely to put a lot of effort into protection from cyberattacks because they consider themselves too small to be targeted. While the potential gains of attacking smaller companies may be less impressive, the task is usually less difficult and more dangerous.

What can you do to avoid being targeted by cybercriminals? Consider these tips.

1. Keep all software updated and regularly patched

One of the most common ways hackers gain access to computer systems is via code defects (known as exploits). Some exploits remain unnoticed for years before they are patched, so if you do not update regularly, you could leave your networks vulnerable to anyone with a little bit of technical knowledge. Exploits can affect all software, from operating systems and browsers to specialized software and more.

2. Invest in a reliable VPN

A VPN (virtual private network) creates a secure connection over a less-secure network between your computer and the Internet. A VPN makes you essentially invisible to hackers so they cannot steal your passwords or financial information or track your activities.

There are many VPN options available. Before you choose a service, determine your organization's needs and carefully research which one is the best fit.

3. Educate and train your staff

Do you know what the biggest vulnerability in cyber security is for most businesses? If you guessed "employees" or "employee negligence," then you are correct. Employees (in house and remote) represent the most significant security risk to businesses and employee negligence is the leading cause of data breaches, according to research from Shred It.

Cyber awareness training provides a basic understanding of cyber security best practices. Great training teaches employees — everyone from C-level executives to the janitorial staff — how to:

- Identify and respond to phishing and other email scams (hint: don't engage with them).
- Practice safe internet habits (such as creating secure passwords and not using them across multiple accounts).
- Familiarize themselves with your organization's cyber security-related policies and abide by them.
- Recognize social networking threats.
- Safely collect, store, manage, and send client and company data.
- Comply with government and industry regulations.

Your employees are your company's first line of defense. While automated cyber security protections such as firewalls, antivirus and antimalware solutions can help, they do not block every threat. This means that your employees need to be able to recognize and act quickly (and safely) to threats that make it through your network and other systems' defenses. They also need to know how to not create risks by handling sensitive data and information appropriately.

Effective cyber security training for cyber-crime prevention is educational for both your employees and your IT security staff. Though we already know the way that it is educational for the former, the way that it is also educational for the latter is that it should involve regular testing as well. This training helps info sec professionals assess what is or is not working from the training so they can identify areas they need to drill down on more in-depth to increase employee understanding. One example of such testing, phishing simulations, will be discussed in a coming section.

4. Divide, encrypt, and back up sensitive data

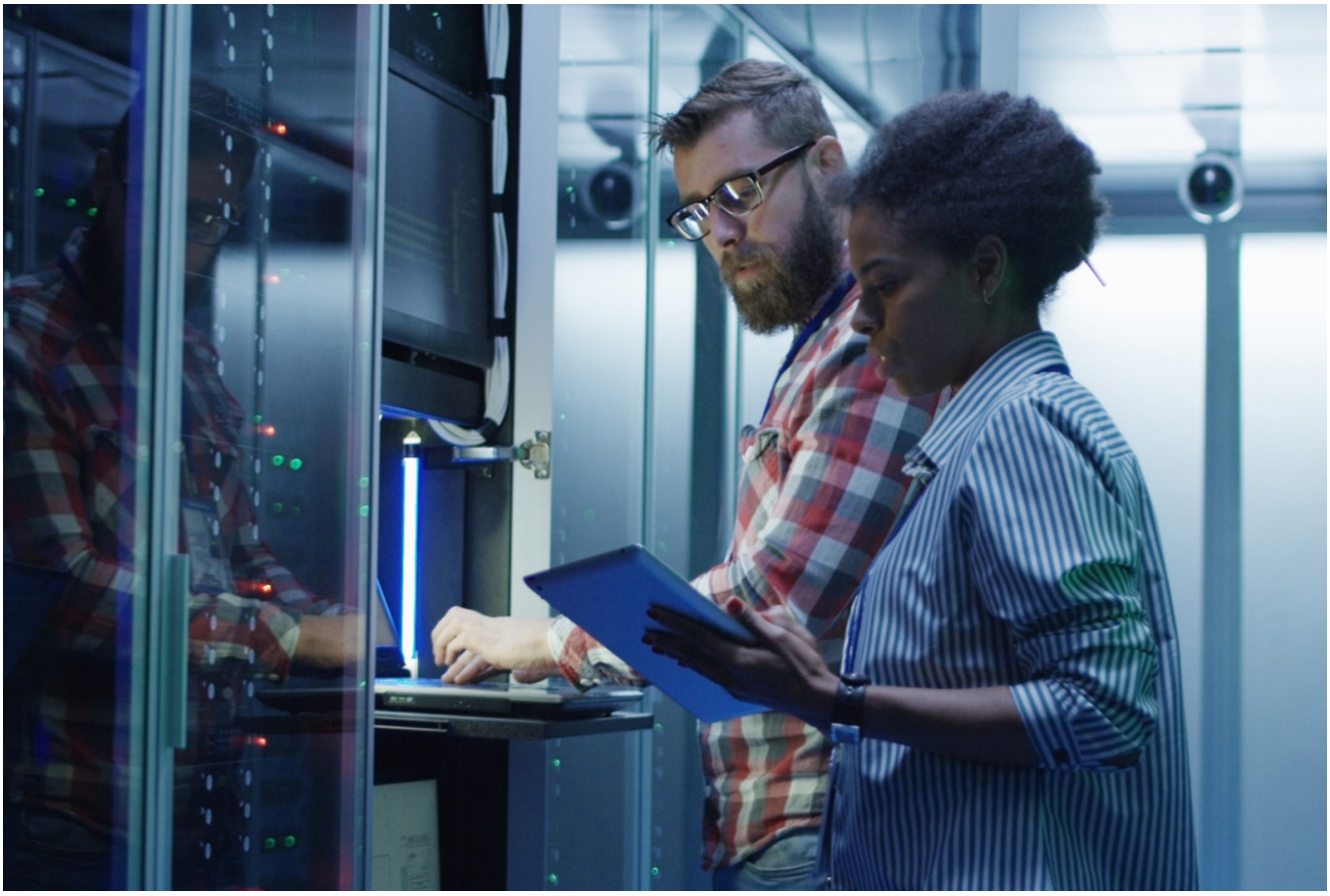
Today, data is a business's most critical asset; protecting it should be a top priority. Put it behind as many layers of security as possible. Do not keep it in a single source, divide it into segments. This approach may be less convenient, but in case of a security breach, hackers will not get access to your entire data bank. Use advanced encryption methods to make sure that even if information gets stolen, hackers will not be able to use it (and make sure your encryption software always has the latest update).

Finally, back up your data regularly. Cloud solutions such as Backup as a Service (BaaS) and Disaster Recovery as a Service (DRaaS) are the most efficient ways to ensure that this happens.

5. Set up strict limitations on company computers

Make sure your employees cannot install unauthorized software on company computers without approval from your system administrator. This will help prevent malware from infecting your company's network and reduce wasted time.

These days, cybersecurity can no longer be treated as an afterthought. A security breach can be catastrophic for any business, even those without a strong digital presence. The only way to protect yourself is to prepare and follow the advice above.



6. Use anti-virus software and keep it updated

Using anti-virus or a comprehensive internet security solution is a smart way to protect your system from attacks. Anti-virus software allows you to scan, detect and remove threats before they become a problem. Having this protection in place helps to protect your computer and your data from cybercrime, giving you piece of mind.
If you use anti-virus software, make sure you keep it updated to get the best level of protection.

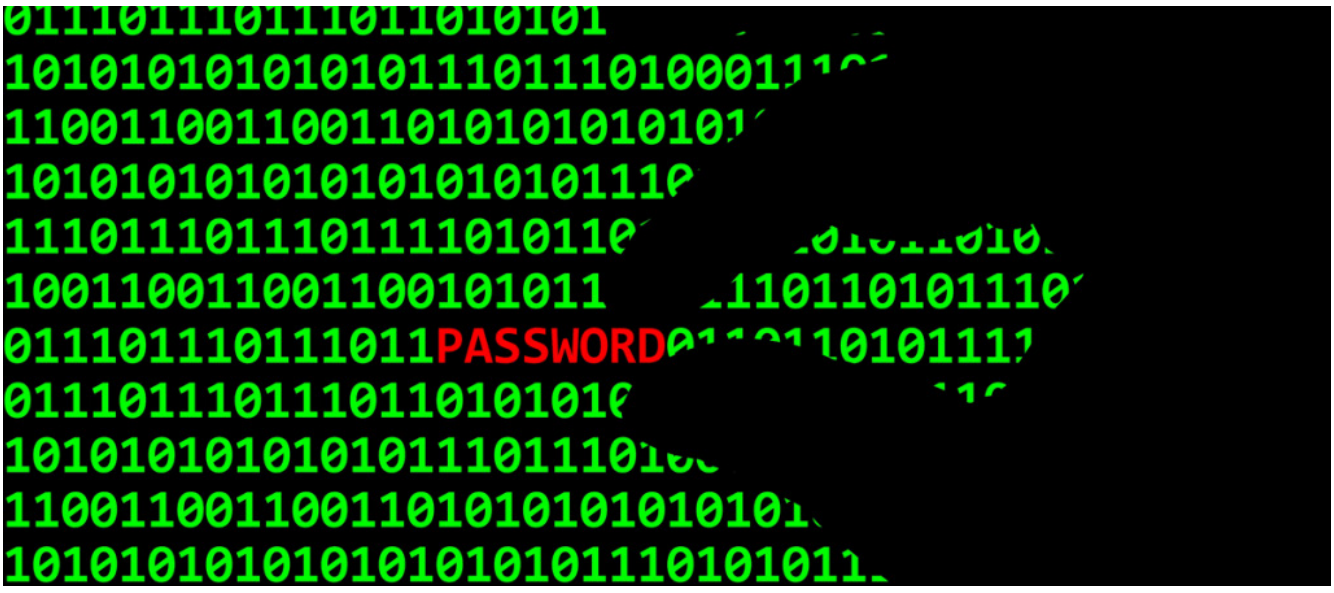
7. Use strong passwords

Be sure to use strong passwords that people will not guess and do not record them anywhere. Or use a reputable password manager to generate strong passwords randomly to make this easier.

In many instances, automated processes are used to crack passwords. These processes are called brute force attacks. There are several different types of brute force attack:

- Hybrid brute force attacks. You may have heard of dictionary attacks. These are one of the most common forms of brute force attack and use a list of words in a dictionary to crack passwords. Other types of attack may use a list of commonly used passwords. If your password is 'password' for example, a brute force bot would be able to crack your password is seconds.
- Reverse brute force attack. Reverse brute force attacks do not target a specific username, but instead, use a common group of passwords or an individual password against a list of possible usernames.
- Credential stuffing. When a username and password pairing is known by the attacked, they can use this information to gain access to multiple websites and network resources. For example, many users choose the same password to access many different websites for the sake of simplicity. Taking precautions like using two-factor authentication and using different passwords for every different network resource can help prevent brute force attacks that rely on credential stuffing.

Brute force attacks typically rely on weak passwords and careless network administration. Fortunately, these are both areas that be improved easily to prevent vulnerabilities that could bring your network or website resources to their knees. For example, utilizing strong passwords, allowing a limited number of logins attempts and enabling two-factor authentication can help prevent brute force attacks.



8. Two-factor authentication

Two-Factor Authentication (2FA) is sometimes called multiple factor authentication. In simple terms, it adds an extra layer of security to every online platform you access. The first layer is generally a combination of a username and password. Adding one more step of authenticating your identity makes it harder for an attacker to access your data.

Most 2FA systems are designed to ascertain one of three factors

- Something you know,
- something you have, or
- some part of your body.

The second layer could ask for the name of your cat, a secret code sent to your phone, or a fingerprint scan. Or it can include combination of more than one or even all three of them. That is the reason for calling it sometimes multiple factor authentication.

Regardless of the nature of the second layer, it serves as a vital barrier to your account.

Passwords have been the mainstream form of authentication since the start of the digital revolution. But this security measure is far from infallible. Here are some worrying facts about this traditional security measure:

- 90% of passwords can be cracked in less than six hours.
- Two-thirds of people use the same password everywhere.
- Sophisticated cyber attackers have the power to test billions of passwords every second.

The vulnerability of passwords is the main reason for requiring and using 2FA.

9. Follow industry best practices and guidelines

Cyber-crime prevention is not a one-size-fits-all approach. Organizations of different sizes have different needs, threats, risk tolerances, vulnerabilities, and capabilities. Luckily, governments, regulators, and even industry organizations have provided some general frameworks and security recommended practices for organizations to follow to reduce their likelihood of falling victim to cyber security attacks. However, it is important to note that some are more particular than others in their recommendations or requirements. For example:

- GDPR, which stands for General Data Protection Regulation, is comprehensive legislation that rolled out in 2018 to protect the data and privacy of European Union citizens (even those living abroad and international companies that handle data of EU citizens). The regulation outlines much of what is or is not allowed, states what falls under data subjects' (the citizens') expectations of privacy, and details some of the stiff penalties that businesses and organizations alike could face for noncompliance.
- NIST, also known as the U.S. Commerce Department's National Institute of Standards and Technology, is the go-to resource for cyber security professionals NIST released version 1.1 of its popular Cybersecurity Framework document, which outlines ways to improve cyber security for critical infrastructure. The goal of the document is to provide "a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls that may be voluntarily adopted by owners and operators

of critical infrastructure to help them identify, assess, and manage cyber risks." Ideally, the framework should be used to complement your organization's existing cyber security program and risk management processes, not replace them, and outlines five concurrent and continuous "functions"— Identify, Protect, Detect, Respond, and Recover — to address cyber security risks.

- HIPAA, the national Health Insurance Portability and Accountability Act in the United States, is not as particular nor stringent as the GDPR about how patient data and confidential personal health records are to be used, stored, or transferred. HIPAA's Security Rule does not technically require encryption of patient health information (PHI). Instead, § 164.312's standard for transmission security says that organizations must "Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network." Even the rule's technical safeguards concerning the topic of encryption are defined only as "addressable" requirements — handlers of PHI must "Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate." Isn't that comforting? Granted, the language is left purposefully vague to account for evolution and changes in technologies. However, it also leaves businesses with potential opportunities to argue away their way out of responsibility and accountability.
- PCI SSC, the Payment Card Industry Security Standards Council, requires businesses that use account data to implement certain protections for that information. These data security requirements, known as the PCI Security Standards, require encrypted transmission of cardholder data across public and open networks, use of strong access control measures, implementation of a vulnerability management program, and more. Failure to comply with these standards can result in significant fines and penalties — not to mention possible suspension of your company's card payment processing capabilities.

Sounds simple enough, right? These are highly regarded resources for IT security professionals and businesses alike. The trouble is, though, not all businesses adhere to these recommendations (or, in some cases, required practices). An apropos analogy is when an adult tells a small child not to touch a hot stove because they will get hurt, yet the kids does it anyway: Some children (or businesses, in this case) choose to learn the hard way and wind up getting burned. For companies who instead choose to "listen to the adult" and adopt these required or recommended methods of cyber-crime prevention, they will be in a better position to protect their data, employees, and customers from cyber security attacks and data breaches.

10. Implement email security solutions and phishing simulations

Considering the rise in business email compromise, phishing, and other email-related concerns, the modern virtual mailbox represents a significant area of cyber security vulnerability. Unlike physical messages sent by a physical mail carrier, emails can contain a variety of threats from attachments containing malware (often Microsoft Office files such as Excel spreadsheets and Word documents) to embedded links that direct users to malicious websites. Many businesses tend to rely on the anti-spam filters that come with bundled with their email platform or antivirus programs to protect their business's communications. However, there are additional third-party email solutions that you can use such as anti-phishing platforms and email signing certificates.

Anti-phishing platforms can automatically identify and even quarantine potentially dangerous emails so users can't engage with them. Some anti phishing solutions even provide an educational component to help users understand why emails are being quarantined (such as a sender's name not matching their email address or signature, embedded links directing users to dangerous websites, etc.). Email signing certificates allow users to digitally sign and encrypt emails containing sensitive or confidential information to avoid man-in-the-middle (MitM) attacks and eavesdropping. By signing your emails, it allows your recipients to authenticate that you are you and mitigates email tampering.

While putting these protections in place is exceedingly important, you still need to take it a step further and conduct periodic phishing simulations. This will allow you to test the cyber security awareness of your employees to assess how well they can apply the lessons from your training in real-life scenarios. Seeing whether employees are approaching email more judiciously or are opening every message with wild abandon will help you recognize which employees are your biggest risks as well as identify new areas to address with cyber security and phishing awareness training.