PRODUCTIVITY AND CYBERSECURITY

How improving your productivity can make you more cyber secure

THIS MONTH'S TOPICS:

Statistics reveal a concerning trend: fatigue and burnout significantly increase the likelihood of cybersecurity lapses. From mismanaged passwords to overlooked phishing emails, tired minds are a cybercriminal's playground.

In the fast-paced digital landscape, productivity isn't just about doing more in less time; it's about smart, secure, and sustainable practices that keep our data safe and our minds clear.

In this month's newsletter, learn how cybersecurity and productivity connect, and dive into the habits you need to implement in order to be more secure.

WHY PRODUCTIVITY?

Productivity is not just about doing more but doing so in a manner that sustains energy and sharpens focus, thereby enhancing cybersecurity practices.

The Problem: Fatigue and Burnout

Recent studies have highlighted a concerning trend: cyber fatigue and burnout are not just affecting our physical and mental well-being but are also making us more vulnerable to cyber threats. Tired employees are more likely to overlook phishing emails, use weak passwords, or bypass security protocols, inadvertently opening the door to cybercriminals.

43% Of employees admit to sharing login information with others to avoid stress, as well as avoiding their work if it involved logging in.

88% Of security professionals have seen a breach caused by burnout or fatigue.

Improve Your Productivity

While cyber fatigue is part of a typical workday for many, one way to combat it is by increasing productivity. Think about it: when you are more productive, you're more able to take breaks and have the time to think critically before making decisions. To increase productivity:

- Watch short trainings on how to leverage the tools your company provides.
- Search for trusted tools that allow you to complete your work more efficiently.
- Make a to-do checklist and focus on one task at a time.

Efficient Cybersecurity Tips

Tools for increased productivity

Password Managers

Password managers store and autofill complex, unique passwords for each account, saving time during the login processes and reducing the downtime associated with resetting forgotten passwords.

Short Training Bursts

Incorporate short, focused learning sessions on cybersecurity topics and other topics relevant to your role. These bite-sized educational bursts can enhance your productivity and your response to cyber threats. One way to do this is by watching weekly training videos in the portal.

Multi-factor Authentication

We know what you're thinking- implementing MFA doesn't make you more productive, it adds time to your workday. However, these extra seconds logging in are miniscule compared to the amount of time you would have to spend recovering a compromised account, or dealing with the fallout of identity theft or a data breach that could occur if your account is easily accessible.

SCAM OF THE MONTH

Each month we highlight a scam that demonstrates tactics criminals are using RIGHT NOW, to better prepare you when the next scam hits.

Danny works in IT. He has been at his new job about three months. His company had been working hard to get him up to speed on all of the different platforms and tools they utilized. They provided Danny with a four-hour video that explained how to use these platforms. One of them was a cloud storage system that Danny was unfamiliar with. He let the training slide for the time being as he had many other things to do.

He didn't realize just how important the cloud storage system was. It housed all the company's important files and their clients' files. When Danny's computer started working slower than normal, he assumed it had to do with the thousands of files in the cloud storage. He decided to delete most of the files, assuming they were just copies of the real files. He ended up deleting over 100,000 files, videos, and records that were crucial to the business and their clients. The company had not backed up the files in a secondary location, so the files were lost for good.

Did you spot the red flags?

- Danny should have taken the training videos before interacting with the cloud platform.
- He also should have checked with a supervisor before deleting files from the platform.
- The company should have had the files backed up on a separate location to avoid these issues. They also could have limited employees' access to important documents, only allowing access to those needed for the role.

Insider threats are not always malicious. In this case, the company lost a huge amount of important data because of a mix of cyber fatigue and lack of training. While sometimes long trainings are necessary, if the employee could have watched quick training videos over a longer period of time on the platform, he could have reduced stress, increased productivity, and avoided this mishap.

While cloud platforms serve as great locations to store files, it is still important to backup these documents or have copies stored in another secure location.

CYBER NEWS

News and cyber lessons from March

MARCH
2024

IMPERSONATION OF NEWS OUTLETS

A fraudulent operation has been discovered impersonating dozens of legitimate news websites. The scammers created domains similar to those of real news outlets like BBC, CNN, Forbes, Canadian News Today, Australian News Today, and many other popular outlets around the world. They then copied the design and news stories from legitimate websites to trick companies into paying large fees for ad space. These websites could be used to spread fake news. They also could be advertising fake products or other fake websites.

UPDATES & EVENTS

-March 31st is World Backup Day. To celebrate, make sure all of your data, especially sensitive and important data, is backed up in a secure location.

HACKERS IMPERSONATE GOVERNMENT AGENCIES

A group of cybercriminals are carrying out a business email compromise (BEC) scam where they impersonate government agencies. Their scam often includes malicious links or QR codes in attached PDFs. If these links are followed, the user is taken to a fake website mimicking a government agency or they are prompted to enter their Microsoft credentials. Then the cybercriminals use the exposed credentials to infiltrate the users' organizations. Proceed with caution when you receive out of the blue messages from government agencies.