Monthly Cyber Quick

Newsletter

November 2022 Issue #1

What should you do when you lose hours of work?
Discover a virus? Get hit with ransomware?
We have answers to ALL your tech questions!

THE CYBER-SECURITY BLANKET YOU NEED FOR WINTER!

Bringing you the monthly scoop on information security.

From the tricks hackers are using against you right now, to the best digital defenses available, to small ways you can protect your accounts every day, we're here to bring you up-to-date news on cyber-safety!

"Are they Samoas?"

THE MORE YOU KNOW

Did You Know?

The brand that is most commonly faked by phishers is LinkedIn, according to the Q2 2022 Brand Phishing Report from Check Point Research. Scammers often imitate real brands to coerce you into giving out private information. In 2022, phishing scams have impersonated LinkedIn approximately half of the time.

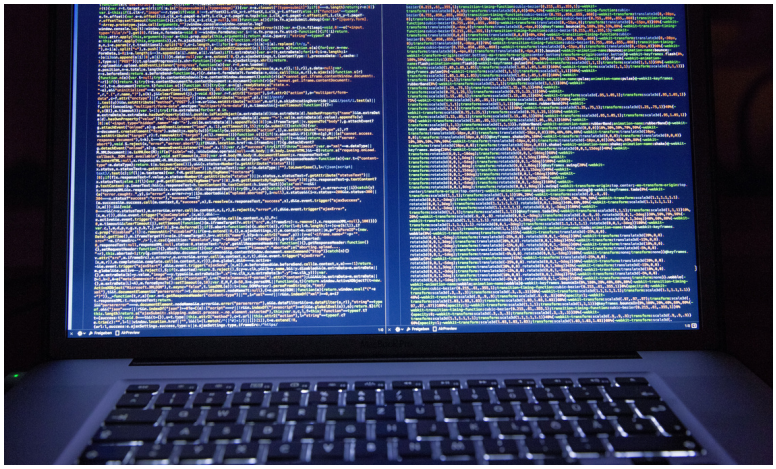
Does that mean you should only stay wary of emails from LinkedIn? Of course not! Cybercriminals target specific groups depending on their scam, where they got your information, and what websites or businesses YOU are most expecting to hear from.

Everything You Need to Know About PII

Annual refreshers and updates to your existing cybersecurity knowledge is really the best way to keep your network safe on a day-to-day basis. With that comes the protection of all the data you have on there, including PII.

You've probably heard your I.T. department mention it before...or hopefully it sounds familiar from your regular security awareness training. PII, or **personally identifiable information**, refers to data which ties back to a specific individual, in this case yourself.

How much do you really know about this important term, and keeping it secure on a daily basis?

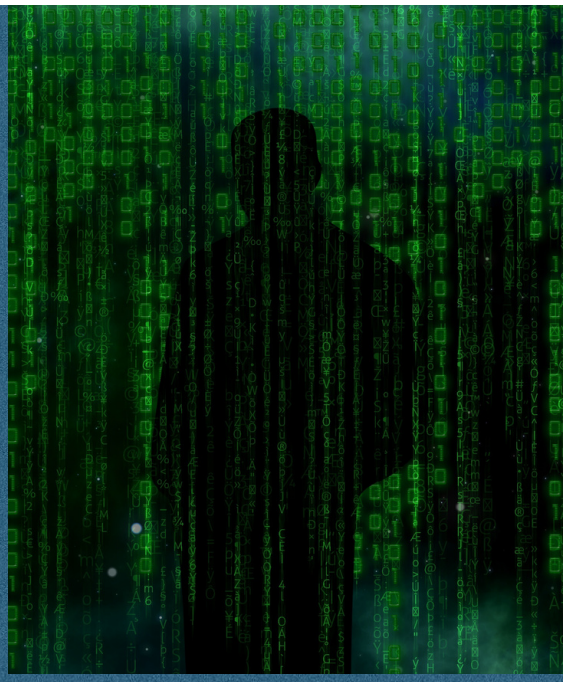


Things like your name, home address, phone number and Social Security number are all different types of PII. If your friends or parents ever told you not to give out your real name or number online, they were trying to protect your PII from becoming a target for threat actors online and in real life.

Real-World Example of PII Theft

700M LinkedIn accounts experienced any Internet user's worst fear: their personally identifiable information (PII) ended up for illegal sale in June 2021. Cybercriminals acquired email addresses, full names, phone numbers, locations, login credentials and connected online accounts of over 90% of the user base (at the time - they've since grown by over 50M users). The criminals illegally scraped data using LinkedIn's own API tool and posted the information to the Dark Web.

In this situation, it's not as though LinkedIn could erase the stolen data off the Internet once it was out there! As the saying goes: once it's online, it's out there forever. This situation highlights how important it is to understand the tech you use so as to close zero-day vulnerabilities before they are exploited. It helps to perform security updates ASAP, too!



The Lesson

For your safety, hide your identity online! If you run into trouble, hopefully you have been performing regular backups or have cyber-insurance at your back.

Automate your cybersecurity processes so you can focus on the elements of cyber-safety that need a human touch, like recognizing convincing phishing messages and multi-factor authentication.

- PII is the most expensive data to lose in a breach; hackers sell it, buy goods on your accounts, or extort you directly!
- PII theft makes up 44% of cyberattacks, making it the most commonly compromised type of data
- Criminals can sell your private information for hundreds of dollars on the Dark Web, selling for an average of about $200 per record
- In 2021, breaches that compromised credentials cost a total of over $4M

How to Spot Malicious Files

Entire industries have cropped up to distribute digital files. Remember LimeWire? It was a music pirating software that shut down for copyright infringement in 2010, a disappointment to its base of 50M monthly users. That was over a decade ago, before the Internet became the widespread phenomenon that it is today. This number reflects how popular file downloading is and always has been, which is why expert advice to just "not download random files" often falls on willfully deaf ears.

The fact of the matter is, it's convenient and fast to get pictures, documents and anything you want off the web, where people both altruistic and ill-motivated share them for free.

Your online safety rests in YOUR hands! Learn how to spot the difference between malicious and benign files when you find them out there on the Internet.

Pro-Tip: Don't Pay Ransomware

More than 90% of ransomware victims who pay don't get access to their files again.

Even if you pay, it may not be enough: Double extortion happens when a ransomware demand is then followed up by a second fee request, this time to prevent the hacker from leaking all that information they found on your computer. Even when it's safely back in your hands, your data isn't protected from the public eye or hungry bidders on the Dark Web.

Hackers make their fortune by breezing past your bare-minimal security measures and get into the accounts that really matter. That's why equipping all of your Internet-connected devices with auto-scanners and firewalls helps detect unusual network activity so you can take more immediate action against the intruder.

Two-factor authentication requires you to verify your identity through some unconnected means, so even hackers can't seize your accounts even with your password. Instead, you'll get an alert about an attempted breach and know right away that something isn't right.

Your PII personal identifiable information should be your most safely guarded secret online. It can be weaponized against you, sold to a scammer or used to extort money from you. If gathered PII helps the threat actor narrow in on your real-life location, that poses even more danger. Keep your private data secure, whether you're communicating it online or have the files safely in storage.

Continuous Monitoring Matters!

Automated security systems detect unusual activity on the network based on your habits and security clearance level, then notify you immediately about suspicious behavior.

RESTECH SOLUTIONS

ADDRESS HERE

Top News Inside

Use Web Filters

Whether you're on a mobile device, laptop or something else that connects to the Internet, add web filtering applications to your line of cyber-defense. These programs may seem scary because they ask for access to view online activity and run in the background of all your other apps, but their defensive capabilities are INVALUABLE!

These tools can check domains, URLs, IP addresses and more to warn you of any and all suspicious behaviors. They'll ask if you're sure before going somewhere unsafe so you have time to navigate back to less murky waters.

Avoid EXE Files

You might be familiar with file types like JPG, PDF and DOC. While any of those COULD have malicious code embedded to compromise your device, you should especially beware of files that end in EXE.

Bad actors may attempt to hide the threat by naming it "Example.pdf.exe" or something similar. Give your antivirus software permission to scan attachments and downloads before allowing it onto the machine at all, cutting off potential threats at the start.

Your job might send you .exe files for a legitimate reason. The file type simply indicates that it contains executable code that will launch when you open it. Although you might trust your security provider to send you new software, this attention-to-detail will tip you off to the clear and avoidable danger when a suspicious sender sends you the files.