2nd Quarter Newsletter 2019

PCS TechNEWS

Pittsburgh Computer Solutions
451 Valleybrook Road Suite 200 McMurray, PA 15317 724-942-1337

What is a Keylogger?

Keyloggers secretly record what you see, say and do on your computer. Employers use keyloggers to watch employees, but cybercriminals use them too.

What is a Keylogger?

Did you know that your keyboard could let cybercriminals eavesdrop on you? Or that they could watch you on your system camera? Or listen over your smartphone's microphone?

Welcome to the world of keyloggers, a particularly insidious type of spyware that can record and steal consecutive keystrokes (and much more) that the user enters on a device.

A keylogger may be either hardware - or software - based, and has its uses as a legitimate personal or professional IT monitoring tool. However, keystroke logging can also be used for criminal purposes. More commonly, keystroke logging is malicious spyware that is used to capture sensitive information, like passwords or financial information, which is then sent to third parties for criminal exploitation.

Why Keystroke Logging is a Threat

When you are unaware that everything you type onto your computer keyboard is being recorded, you may inadvertently expose your passwords, credit card numbers, communications, financial account numbers and other sensitive information to third parties. Criminals can exploit information by accessing your accounts before you even know that your sensitive data has been compromised.

Keylogger malware may reside in the computer operating system, at the keyboard API level, in memory or at the kernel level itself. Keylogging can be hard to detect because it doesn't always cause noticeable computer problems, like slow processes or glitches. It can be hard to detect even by some antivirus programs because spyware is good at hiding itself—it often appears as normal files or traffic, and can also potentially reinstall itself.

Continued on next page

How can I tell if I have a keylogger infection?

Keyloggers invade PCs (and Macs, and Androids, and iPhones) in the same way that other malware does. They install when you click on a file attachment that you've been duped into opening - most commonly because you fell for a social engineering scheme or a cleverly designed phishing expedition. The attachments can come to you by email, through a text message, an instant message, on social networks, or even through a visit to an otherwise legitimate but infected website, which exploits a vulnerability in it and drops a drive-by malware download. Also, keyloggers rarely arrive solo. The same Trojan that delivers the keylogger can slip other malware on your system - such as adware, spyware, ransomware, or even a legacy virus.

Fortunately, it is possible to protect your computer from keylogger software. Keeping your operating system, software products and Web browsers up-to-date with the latest security patches should always be part of your security solution, but the best defense is to install a good anti-spyware product that protects against keylogging malware, or a complete internet security solution with strong features to defeat keylogging.

For more information call PCS at 724-942-1337. Protect your business starting today.

So what is whaling anyway?

It's a type of phishing attack, classified under spear phishing scheme as it targets certain individuals. It's directed at CEOs, executives, or others who have access to highly valuable information. Since these individuals may not be deep in the daily operations of a business, they can actually be more susceptible to someone posing as an official via email.

The goal of a whaling attack is to trick an individual into disclosing personal or corporate information through social engineering or a spoofed email. The attackers may send the victim an email that appears to be from a trusted source; leading them to a fake page ready to collect sensitive information.

Whaling Continued

Attackers know who to target. They typically go for individuals with deep pockets or those from an older generation who aren't glued to their phones to receive alerts that their security has breached. By targeting high-value victims, especially CEOs and other corporate officers, attackers may also induce them to approve fraudulent wire transfers using business email compromise techniques. In some cases, the attacker impersonates the CEO or other corporate officers to convince employees to carry out financial transfers.

Whaling attack emails and websites are highly customized and personalized, and they often incorporate the target's name, job title or other relevant information gleaned from a variety of sources. This level of personalization makes it difficult to detect a whaling attack. These attacks can fool victims because attackers are willing to spend more time and effort constructing due to their potentially high returns. Attackers will often use social media, such as Facebook, Twitter and LinkedIn, to gather personal information about their victim to make the whaling phishing attack more plausible.

By responding to this fraudulent act, the executive will likely discharge embedded codes that gives these criminals access to their networks where they work on or store their highly-regarded data and through this, they can remotely control an executive's computer or log their keystrokes and in a few days, can access personal data and company passwords. This could mean huge losses not only to your business but to one's self as well.

Regardless of whether you're a C-level executive or one of the many minnows in the pool, data security is important. Everyone in a company can benefit from security training in order to stay on top of ever-changing threats.

PCS recommends that the only way to mitigate whaling problems is to educate their senior management staff as well as their finance teams but still this isn't enough. Enforcing secondary layer of confirmation of any suspicious requests would also be a reasonable solution.

If you ever encounter one, don't hesitate to call PCS at 724-942-1337 for any assistance. With the right awareness training and security measures, this is just one way that we can get ahead of these cyber criminals and avoid getting "phished".

Security Awareness Training

You might not think you need to educate end users about cyberattacks, compliance issues, and other risks they face online.

Every business is a target. And there's a reason regulated industries like healthcare, finance, energy, and others require Security Awareness Training for end users.

Security awareness training is rapidly increasing in popularity because it's becoming a necessity to ensure businesses of all sizes are secure. The type and depth of training may vary, but all offerings should incorporate basic phishing simulations and relevant data-compliance and security courses that educate users on the dangers they face both at work and at home. As these training offerings increase in sophistication, you can espect to see not only highly customized content by industry sector, but also content geared to the actual real-life security incidents and behaviors of individual users.

Security awareness training is a layer of defense that has often been treated as a burden, but is now seeing serious advances—particularly as it sheds its standalone nature and is embraced by organizations small and large as an essential form of protection.

Of course, security awareness training is only one layer of defense. As such, it cannot deliver 100 percent protection, but it does help minimize an increasingly dangerous IT security issue—user error—and it educates users to make wiser decisions online, whether in the office, working remotely, or on their home networks.

Awareness and data security are becoming more and more important for small businesses. The more data you collect about your customers, the more important this becomes. Collecting and saving a customer's personal information can make you a target.

Also if your customer's information is compromised, it can make them a target as well. If an evildoer gains access, it may allow them to open a new cell phone account with your customer's information, apply for a credit card, or otherwise steal their identity.

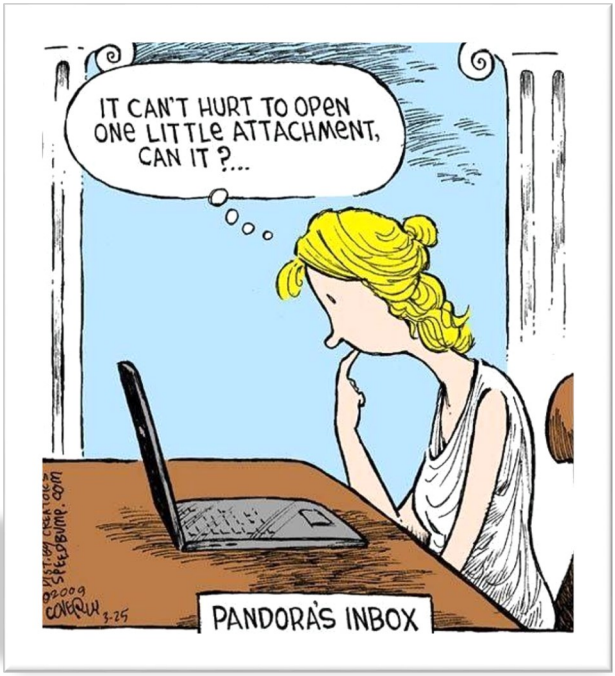
Data breaches are commonplace, unfortunately. Most of us have read the headlines describing data breaches at large companies. The reality, however, is that hackers target small and midsize businesses in greater numbers. In 2018 alone, 58% of all cyber attacks affected small businesses. Why? Cybercrime is first and foremost a numbers game. The majority of cyber attacks do not target specific companies. Instead, hackers look for vulnerable computer corporations. Without such security protocols in place, small and midsize businesses are especially defenseless, particularly when it comes to social engineering scams like phishing.

As hackers develop new methods to get your data, you need to keep up with the latest techniques to keep your business safe.

Have a Data Security Awareness Training Program in Place

Data security awareness and education are key for businesses of all sizes. Just because you're not a large corporation doesn't mean you're safe from attacks. New threats and new technologies are always emerging. While you can mitigate some of the risk through best practices, your security chain is only as strong as its weakest link. A regularly scheduled training program help keep your staff up-to-date on the latest social hacks, phishing attempts, and physical breaches to reduce human error.

PCS can help your business provide security awareness training for your staff, no matter how many people you employ. Training can take place as a group activity or individually as your staff's work schedules allow. As threats continue to evolve, you want your staff to be able to protect your company's data assets. Ongoing training can help your staff to be better informed and more prepared for what may lie ahead.



For Assistance with Security Awareness Training
Contact PCS at 724-942-1337

PCS Referrals

We think PCS customers are really great and from what we've been hearing a lot of, the feeling is mutual. Our referral program enables us to give something back to our clients who continually support and trust in our service.

It's pretty simple. When you refer a small to mid-size business in need of IT support, we'll send you a PCS Referral t-shirt! If your referral books an appointment with us, you'll receive an item of your choosing from the following selection: *PCS growler, gift basket or an Amazon gift card. (Each item valued at $50)*

Better yet, if your referral becomes a PCS client, you'll receive an Amazon gift card valued at $100. It's our way of saying thanks for being a loyal customer.

How To Submit Your Referrals

Email PCS at: shaas@pcsmsp.com

Call: 724-942-1337

Follow & Like PCS on Facebook: Message Us

https://www.facebook.com/pittsburghcomputersolutions/