Recognizing a Cyberattack: Save Your Data by Looking for These Signs

By Kelly McNeil, TechBldrs, Inc.

It may not have hit the headlines like the Coronavirus or election season, but the United Nations recently suffered a major security breach. A vulnerability in their system — caused by a failure to patch a known problem! — was exploited by hackers to hit a variety of targets worldwide. What does the fact that the UN is lagging behind on necessary cybersecurity precautions mean for the rest of us?

Software manufacturers spend millions of dollars a year on patching security flaws and releasing those fixes to their customers. The hole in the UN's security should have been patched by their IT staff within a month of the release of the patch, but it wasn't. Instead, the UN was left wide open to the attack, which was likely orchestrated by an organized group of hackers, and could likely have been helped along by someone within the UN clicking on something they shouldn't have. The extent of the breach remains unknown, but reports suggest that the thieves made off with a catastrophic 400GB of data to now do with what they please.

This is a situation caused by negligent IT support — but could an employee have helped stopped the breach in its tracks by recognizing a few key signs?

Here's how you recognize a cyberattack in progress, and here's what you can do to try to limit the damage it does.

1. A strange email: Sometimes an email will just look "wrong" to you — whether it comes from an unknown sender, or asks you to accept a payment you never requested, or any other suspicious activity, trust your gut! If it was supposedly sent by someone you know, give them a call or talk to them in person to confirm. Don't click on any links, open any attachments, or reply to the email, just delete it before a hacker uses it to cause damage.

2. A suspicious error message: Sometimes it's the entire screen, sometimes it's just a window, but an error message you don't recognize and doesn't look "official" is never good. When it doubt, don't click on anything, just crash your system: hold down the power button of your computer until it shuts off, or pull your computer's plug out of the wall. Crashing your system will power down your computer and stop an attack in its tracks.

3. Calls or emails from a service provider: Always verify calls or emails from Microsoft, your bank, or any other service provider you use. Hackers who already have some of your information may try to swindle you into giving them more than what they have by impersonating a trusted company, like Netflix, American Express, or Facebook. If something doesn't seem right, hang up/don't click on anything in the email and contact the company's support service to confirm if the person that contacted you was really working for them or not.

4. You're locked out of your computer, but you don't remember trying to logon: If a hacker has your username and/or password (or any you've used in the past), they'll often try to brute force their way into your computer to gain access to your information. In other words, they'll keep trying over and over to guess your username and password combination in hopes that they'll eventually guess correctly. Your computer may lock them out after a certain number of tries, so if you find yourself on the receiving end of a "too many login attempts" error message, hackers may be trying to gain access.

5. Unknown software appears and/or begins installing without your permission: Hackers will often install spyware or other malicious software on your computer once they've gained access. Or it may download automatically after you've clicked something you weren't supposed to! If you don't recognize a program that's running on your computer, or something you haven't authorized begins to install, immediately power down your computer.

6. Your email suddenly stops working: If it's been a suspiciously long time since you've gotten an email and emails you've sent are appearing as unsent, it could be a sign that someone else has access to your account. If you think this might be the case, it's time for a cybersecurity professional to help you — they can determine if it's any cause for concern, or if your email's just on the fritz.

7. Your mouse/cursor moves intelligently on your screen on its own: While we've all seen our mouse move when we bang our knee on our desk, one of the surefire ways to tell if someone's actively accessing your computer is if your mouse is moving like it suddenly grew a brain of its own. Clicking on folders, accessing files, or opening your system settings are all signs that someone else is using your computer. If you ever see this happening, immediately power down your computer and call in professional help.

While remaining vigilant and educated about cybersecurity is your best line of defense against hackers and other criminals, we always recommend calling us if you think you've been on the receiving end of these (or any!) signs of cyberattack. If the UN can get hacked, so can you, and so can your business.

How to Address the Challenge of Cyber Security

Provided by Schultz Technology

Cyber security presents one of the most challenging scenarios for society and businesses in the modern world. In the age of cloud computing and constant online devices, the stakes have never been higher to protect against unknown threats. Cyber security is important with all types of businesses collecting, processing, and storing ever-increasing amounts of data on computers and other devices. A significant portion of that data can be sensitive information, whether that be intellectual property, financial data, personal information, or other types of data for which unauthorized access or exposure could have negative consequences. Organizations transmit sensitive data across networks and to other devices during the course of doing businesses, and cyber security describes the discipline dedicated to protecting that information and the systems used to process or store it. As the volume and sophistication of cyber attacks grow, companies and organizations need to take steps to respond with proactive long-term changes to enhance their cyber security awareness to protect their sensitive business and personnel information.

Recent polls of more than 2,000 security experts employed around the globe present upwards of 90 percent respondents believing their organizations are vulnerable to internal and external threats. Industries from high profile banking to small mom and pop shops are equal to unknown domestic and foreign attacks.

The rate of change we see in IT has brought advancements in cyber security to allow artificial intelligence (AI) driven mitigations through software. AI driven cyber security solutions never tire. They do not switch shifts or have an off day; they work behind the scenes to monitor and mitigate any detected threat. These threats have been taken priority in terms of responsive action — So much so that the FBI now ranks cybercrime as one of its top activities. Companies' personnel are at the forefront of these protections, and without the proper training and investment into cyber security, one wrong mouse click can take an entire business down.

Schultz Technology recommends a top-down approach to cyber security in which corporate management leads the charge in prioritizing cyber security management across its business practices. The National Cyber Security Alliance advises that companies must be prepared to "respond to the inevitable cyber incident, restore normal operations, and ensure your company assets and the company's reputation are protected."

NCSA's guidelines for conducting cyber risk assessments focus on (a) identifying your organization's most valuable information requiring protection; (b) identifying the threats and risks facing that information; and (c) outlining the damage your organization would incur should that data be lost or wrongfully exposed. Cyber risk assessments should also consider any regulations that impact the way your company collects, stores, and secures data, such as PCI-DSS, HIPAA, SOX, FISMA, and others.

Following a cyber risk assessment, your company should develop and implement a plan to mitigate cyber risk, protect your most valuable information outlined in the assessment, and effectively detect and respond to security incidents. This plan should encompass both the processes and technologies required to build a cyber security program. While it may seem like a daunting task, start small and focus on your most sensitive data, scaling your efforts as your cyber program matures.

By shifting the focus from an unknown practice to industry training and from theoretical to practical applications, Schultz Technology advocates the correct employee behavior at the right time to meet the challenge of cyber crime. Our services instrument secure, meaningful protection.

For additional information, please call 610.495.6204 and visit www.schultztechnology.com.