The IT Insider

July 2018

HOW TO IDENTIFY CYBER THREATS AND PREVENT THEM

There are no number of security systems that can stop every attack.The severity of the attack, then, is determined by how well a company can respond to threats they detect, and how quickly they can recover afterward.

Know the threats, take practical precautions, and have a recovery plan in place.

This is the harsh reality of cybercrime.

Because cybercriminals are always one step ahead of security measures, we have to adapt. This means we need to have the right tools in place to identify potential threats before they become serious. These tools save companies millions in potential damage to both reputation and revenue. They are beyond anti-virus. They alert for threats that make it through the anti-virus wall.

Outside of these reporting tools, which any good IT support company should use (Ask yours about their proactive monitoring tool!) the trick to cybercrime prevention is making yourself a difficult target. It takes mere minutes for most cybercriminals to crack a password or find a weak spot and access a company's database. If you can increase your security and know-how and make it more difficult for the hacker, they may move on to easier targets.

So, how do you do this? Here's a breakdown.

Educating yourself is important, but we've often found that people need to be reminded more than they need to be taught. The tips below should look familiar, but hopefully, they will remind you of best practices you've let fall to the wayside.

Install and update good antivirus. Antivirus software will report when trojans or viruses have been detected. The trojans can act like backdoors into your network -- many hackers rely on trojans to gain full access to your system. If you're getting a steady stream of reports about trojans from your antivirus, it's a clue that your system could be accessed from the outside.

Update your computer ASAP. When you get alerts that it's time for a computer update, get it done. These updates and patches help lock down your system with the latest cybersecurity tools. Unpatched and un-updated computers are easier targets for hackers. Remember, making yourself seem like a difficult target is one of the only ways to prevent an attack.

Pay attention to computer speed. An indication that a hacking attempt or malware outbreak is occurring is reduced internet speed. Hacking will usually cause spikes in network traffic, which then affects speed. It should be noted, however, that good hackers can accomplish their attack without slowing down your computer. Typically, a slow computer means an attack has already occurred, and the virus is slowing your computer down.

Steer clear of suspicious pop-ups. Employees should practice safe web browsing. If a pop-up window does appear, you should avoid clicking on them (even to close out of them). Unknown pop-ups can

Do you have the right plan in place to recover after an attack?

be infected with malware or spyware that can compromise the network. Instead, you should close the entire browser window. If that's not possible, shut your computer down and reboot. The extra time and care you take on this will definitely pay off.

Note unusual password activity. Are you locked out of your system? Have you received an email telling you that your password has been changed without your knowing? These could be signs that your password has been compromised. A security best practice is to make sure that all employees create strong passwords that are changed frequently. For example, we suggest 8 or more characters, a symbol, and a number. We also suggest a change of password every 90 days.

Identify mysterious emails. Emails are the number one way cybercriminals are able to access your computer. Hackers have gotten smart - a lot of the phishing emails they send look legitimate. They could even be sent by someone on your contact list. (That's called spoofing.) How likely would you be to question the legitimacy of an email that comes from one of your customers? Practice safe email protocol and do not open email attachments or click online links that you are not 100% expecting. If you aren't sure the email is legitimate, call the sender to verify. It takes more time but ultimately could save you from an attack. Additionally, you should never respond to emails like this. Replies validate the email address, which means they can go on to attack others, too.

So, do you and your employees understand the risks of a cyber attack? Do you know what to look out for? Do you have the right tools to see a potential cyber attack while it happens? If you do have that tool, do you have the right skills and resources to understand what is happening and stop it? Do you have the right plan in place to recover after an attack? If you've got the plan, do you have the right infrastructure and support to carry it out? We can work with you to create a professional, usable, and strong recovery plan for your company.

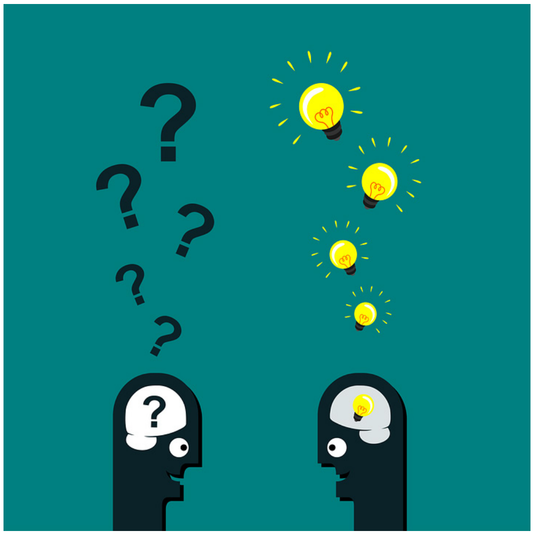
> The extra time and care you take on this will definitely pay off.

FREE CYBERSECURITY AUDIT AVAILABLE NOW

At no cost or obligation, our highly skilled team of IT pros will come to your office and conduct a comprehensive cyber security audit to uncover loopholes in your company's IT security. After the audit is done, we'll prepare a customized "Report Of Findings" that will reveal specific vulnerabilities and provide a Prioritized Action Plan for getting these security problems addressed fast. This report and action plan should be a real eye opener for you since almost all of the businesses we've done this for discover they are completely exposed to various threats in a number of areas.

To get started and claim your free assessment, call our office at 260-440-7377.

> Educating yourself is important, but we've often found that people need to be reminded more than they need to be taught.



THE SOURCE OF KNOWLEDGE IS EXPERIENCE

According to the Small Business Administration, entrepreneurs start 543,000 new businesses each month, but only 18% of them ever succeed. Instead, 46% succumb to incompetence, 30% to lack of managerial experience, 11% to lack of experience in goods or services and 13% to other issues, like neglect, fraud or disaster.

You may notice that three of four of these failure triggers relate to lack of experience. That should be no surprise; after all, there's no substitute for raw experience.

So, I thought it might be useful to put together a list of business axioms to help you shorten the learning curve and get acquainted with the lessons of experience in bite-size form. These are tidbits I've gleaned across years in the business world, pithy ideas that you should examine closely to see if you're utilizing them in your own approach. Here they are, in no particular order:

- Listen carefully to your clients.
- Undercommit and overdeliver.
- Take time to chat with employees; they too, have good ideas.
- A chain is no stronger than its weakest link, so fix or replace it.
- Leaders give more to their staff than just a paycheck.
- If you're going to lose, lose early.
- The person who asks the questions controls the conversation.
- Great leaders take joy in the successes of those under them.
- Praise loudly and blame softly.
- Always push yourself to make continual improvement.
- Arrogance kills success. Don't let your own arrogance blind you.
- When you go the extra mile, people take note.
- You can never achieve greatness without a little discomfort in the process.
- You will not learn anything while you are talking. Listen closely and talk less.

Hopefully you can gain something from the axioms listed above. Remember, wise people learn from the mistakes of others.

> "Good judgment comes from experience, and a lot of that comes from bad judgment."

PREFERRED IT SECURITY SPOTLIGHT

KNOWING THESE 6 TRICKS WILL HELP YOU AVOID PHISHING ATTACKS ON YOUR BUSINESS

1. No matter what the situation, don't panic or click any links until you know they're legitimate. If you suddenly receive an odd e-mail from a coworker, you're right to be suspicious. Investigate before clicking anything.

2. Keep an eye out for red flags. Hackers will often masquerade as a legitimate party, but many times there will be something off about their e-mail addresses or information.

3. Notify the company that's being impersonated. Find the company that the hackers are pretending to be, contact them and let them know the situation. Also report the phishing attack to your IT support.

4. Share the phishing trick on your social media channels.

5. Alert your friends and family about the attack.

6. Let your business know that phishers are trying to penetrate your network.

Read more tips like this on our blog!

Help Us Out And We'll Give You A Brand-New Amazon Echo For Your Trouble

We think you're great and, quite honestly, we wish we had more customers like you! So instead of just wishing, we've decided to hold a special "refer a friend" event during the month of July.

Simply refer any company with 10 or more computers to our office to receive a FREE computer network assessment (a $1,497 value). Once we've completed our initial appointment with your referral, we'll rush YOU a free Amazon Echo as a thank-you (or donate $100 to your favorite charity ... your choice!).

Simply call us at 260-440-7377 or e-mail us at courtney@preferreditgroup.com with your referral's name and contact information today!

OUR COMMUNITY

Our mission is to build lasting relationships within our community. We do our best to give back to our community whenever possible.

This month, we will be supporting the Arcola Volunteer Fire Department at the Arcola National Truck and Tractor Pull.

We'll have a bunch of merchandise at our booth, all proceeds donated right back to the Arcola Volunteer Firefighters!

Stop by and see us June 28-30. It's always a great time!

preferred IT group

CONTACT US

Fort Wayne 260.440.7377	Warsaw 574.306.4288
Columbia City 260.213.4266	Indianapolis 317.426.8180

www.preferreditgroup.com

6333 Constitution Drive
Fort Wayne, IN 46804

Subscribe to our blog and follow us on social media.