ON THE MARK

COLLINS BARROW

Share now

May 2017

A guide to understanding malware & how to protect your business

Dan Gauthier *is the IT Manager at the Sudbury office of Collins Barrow SNT LLP.*
Julie Chrétien *is marketing coordinator at Collins Barrow SNT LLP.*

In today's ever-changing business environment, digital globalization is aggressively increasing. With the world more connected than ever, it is the dawn of a new era of surging flows of data and information. The growth of the internet and use of digital technology have both transformed and disrupted the world of business. A hyper-connected universe has opened up radical new possibilities, but has also cultivated an increase in cybercrime.

According to the 2016 Norton Cyber Security Insights Report, 689 million people in 21 countries experienced cybercrime in 2016. From year to year, the number of businesses that experience loss from cybercrime is on the rise at an alarming rate.

A robust IT infrastructure is the cornerstone of security management and the first step towards protecting your digital world against cybercrime. In order to lessen your chances of vulnerability and protect your computers and devices properly, it is important you understand the different kinds of threats that exist.

Malware

Short for malicious software, malware is a form of intrusive software intended to infiltrate your computer and damage your system without your consent. Malware is an umbrella term, which covers a wide array of threats including computer viruses, spyware, worms, trojans, ransomware, adware, scareware, rootkits and other malicious programs. Some examples of malware viruses include browser hijackers, such as CryptoLocker, MyDoom, Storm Worm and Slammer.

Advanced persistent threat (APT)

A prolonged, stealthy attack in which an unauthorized person gains access to a network to steal data. APT usually consists of several different attacks.

Spam

Unsolicited bulk commercial email messages sent to large numbers of recipients that consist mostly of advertising.

Phishing

Email messages sent by an attacker disguised as a reputable entity that trick individuals into disclosing sensitive information, such as passwords and credit card numbers.

Spear phishing

An email spoof that targets an individual or group to try to get them to reveal sensitive information. Spear phishing is an email or electronic communications scam targeted towards a specific individual, organization or business. Although often intended to steal data for malicious purposes, cybercriminals may also intend to install malware on a targeted user's computer.

Spoofing

An email message with a fake identity that tricks or deceives you or your system. Email spoofing is the forgery of an email header to make it seem as though the message originates from someone or somewhere other than the actual source. Distributors of spam often use spoofing in an attempt to get recipients to open, and possibly even respond to, their solicitations.

May 2017

A guide to understanding malware & how to protect your business

Ransomware / Crypto

Malicious software that cyber criminals use to hold your computer or computer files for ransom, demanding payment from you to get them back. Sadly, ransomware is becoming an increasingly popular way for malware authors to extort money from companies and consumers alike. There is a variety of ransomware that can get onto a person's machine, but as always, those techniques either boil down to social engineering tactics or using software vulnerabilities to silently install ransomware on a victim's machine.

The following are some suggested steps to follow in order to defend yourself against any type of cybercrime:

1. Invest in a backup solution and perform periodic restores to ensure your system is functioning optimally
2. Show hidden file extensions
3. Filter executables from entering your email
4. Disable files running from AppData/LocalAppData folders
5. Patch or update your software
6. Use a reputable security suite
7. Suspicious? Disconnect from Wi-Fi or unplug from the network immediately

In order to prevent you and your business from becoming part of a cybercrime statistic, it is important to develop cyber security strategies.

Identifying hostile emails can prove to be a difficult task. While some email messages are obvious frauds, others can be so highly effective and convincing they manage to fool even the most experienced and tech-savvy users. To protect yourself against email threats, it is of the utmost importance to be suspicious of all emails and evaluate all attachments and links. The Royal Canadian Mounted Police suggest the following ten cybercrime prevention tips:

1. Use strong passwords – combine letters, numbers and special characters
2. Secure your computer – activate your firewall, use anti-virus software
3. Be social media savvy – make sure your profile is set to private
4. Secure your mobile devices – only download applications from trusted sources
5. Install the latest operating system updates – turn on automatic updates
6. Protect your data – use encryption
7. Secure your wireless network – review and modify default settings
8. Protect your e-identity – enable privacy settings
9. Avoid being scammed – verify the source of the email message
10. Call the right person for help – consult with a certified computer technician

To strengthen your defense against hostile emails and prevent yourself from becoming a cyber victim, follow the stop, look & think rule.

STOP

Confirm the sender

- Do you know this person?
- Are you expecting an email?

May 2017

A guide to understanding malware & how to protect your business

LOOK
Evaluate the subject of the email – look, but don't click

- Is there a sense of urgency?
- Is someone asking you to send money to a friend in need?
- Is the subject vague?
- Does it have threatening language?

THINK
Ask questions

- Why am I receiving this email?
- Is this a valid attachment?
- Do I know the sender?
- What is being requested? (Money, personal information, credit card confirmations)
- Does it ask for personal information?
- Are there any spelling mistakes or grammatical errors?

ACTIONS

- Always have onsite and offsite backups
- Perform test restores
- Invest in antiviruses
- Hover over links to confirm their path
- Educate everyone to be able to identify cyber attacks
- Keep your computer operating system updated
- Implement complex password policies
- Invest time to develop/update internet and security policies
- Report suspicious computer activity to an IT professional
- Never forward suspicious emails to others, not even your IT department

A recent Internet Security Threat report, conducted by Symantec, reported that ransomware attacks are on the rise in Canada. The report globally ranked Canada as the fourth country most commonly hit by ransomware and social media scams. Approximately 1,641 ransomware attacks affected Canadians each day in 2015, according to the report. With cyber-attacks more prevalent, having reliable IT infrastructure is critical. Always err on the side of caution. This may very well save you and your company from bankruptcy.

Resources:

- 2016 Norton Cyber Security Insights Report
- Royal Canadian Mounted Police top ten cybercrime prevention tips
- Internet Security Threat Report by Symantec

Dan Gauthier *is the IT Manager at the Sudbury office of Collins Barrow SNT LLP.*
Julie Chrétien *is marketing coordinator at Collins Barrow SNT LLP.*