Rampart Group LLC
Investigation & Security Services

Tip *of the* Week

Cybercrime in 2018

Why Cybersecurity Will Be More Important Than Ever

2017 brought some of the worst cybersecurity breaches in U.S. history. WannaCry ransomware plagued thousands in a massive global cyberattack, a CIA leak exposed thousands of classified documents, and the largest of all hacks hit the credit rating agency, Equifax, exposing many millions of consumers' personal information.

We anticipate even more sophisticated cybersecurity breaches in 2018, forcing governments and companies alike to focus more on loss prevention.

Here are some 2018 cybersecurity predictions:

1. **Ransomware attacks will continue to evolve.** In 2017, Cyber-criminals held data for ransom and extorted relatively small amounts of money. Expect to see these threats grow as cyber-criminals build on ransomware such as WannaCry, NotPetya, Bad Rabbit, and others and extort larger organizations for bigger ransoms than ever before.

2. **Cloud Computing Security Vulnerabilities.** Organizations are implementing cloud computing at a rapid rate pushing IT security teams to keep up with the increasing pace. Without proper security controls and planning, any organization could be vulnerable to data breaches and even regulatory compliance violations.

3. **Social media will create serious risks for enterprises.** In 2018 we will see social media being used more than ever for sophisticated social engineering attacks on organizations. Cyber-criminals and hackers use these platforms to distribute malware, conduct antivirus frauds, and to initiate phishing campaigns. Organization's social media security policies and training should continually be updated, so employees do not fall victim to these types of attacks.

4. **Email will continue to become an even bigger threat.** Email "spear phishing" was quite effective in 2017, and is only getting worse due to improved sophistication, more precise targeting, and better spoofing techniques. Stringent authentication policies and a culture of cybersecurity awareness will be more important than ever to counter this threat.

5. **Wireless network attacks will increase.** A vulnerable network can allow an attacker to intercept and read Wi-Fi traffic between devices and routers, and in some cases even modify the traffic to inject malicious data. It could also allow attackers to obtain sensitive information from those devices, such as credit card details, passwords, chat messages and emails. Ensure your company's router has the latest security protocols at all times.

As businesses, governments, and individuals all experience more connectivity and digital transformation, companies will have to respond to an increasingly diverse cybersecurity landscape. This means that in 2018, companies will need to adopt a security-first culture at all levels of the organization. Take the time to set in place security and data management protocols; and simulate real-time cyberattacks to improve response time. Companies have Personally Identifiable Information, proprietary files, intellectual capital, medical information, legal documents, and other sensitive information that must be protected at any cost.

Here is a Look Back at Our Top Tips for 2017:

1. Ransomware Can Make Your WannaCry
2. Repeal of Privacy Regulations for Internet Providers – How to Protect Yourself when Browsing the Internet
3. Protecting Yourself from Fraud or Identity Theft
4. Simple Steps for Router Security in Your Home
5. When an Employee Leaves Your Company – Protecting Your Data

Call 1-800 421-0614 or visit us at www.rampartgroup.com for further ideas on protection and security. Thanks for reading!

Kathy Leodler
Chief Executive Officer
kathy.l@rampartgroup.com
(360) 981-2703

Paul Leodler
Executive Vice President
paul.l@rampartgroup.com
(360) 981-3397