February 2017

SecurityAwarenessNews

the security awareness newsletter for security aware people

2016
The Year Cybercrime Won

2016: Timeline of Cyberattacks

2017: The Year We Fight Back!

WHAT DOES THE FUTURE HOLD?

2016 THE YEAR CYBERCRIME WON

2016: What a year! For everyone, everywhere, especially for cybercriminals.

2016 began with a massive cyber-attack on a Ukraine power grid that blacked out most of Western Ukraine. In the months that followed, cybercriminals turned their focus to ransomware, holding hospitals, schools and major organizations across the globe hostage to their demands.

Attacks heated up throughout the summer and into the fall, with companies like Yahoo!, LinkedIn and AdultFriendFinder falling victim to massive data breaches and putting new records of compromised accounts in the books. As if that wasn't enough, the source code for a malware strain known as Mirai was made public for anyone to use, resulting in an onslaught of IoT (Internet of Things) DDoS (Distributed Denial of Service) attacks via everyday internet-connected devices such as security cameras and DVRs (Digital Video Recorders).

In a few words, the cybercrime pandemic is paying off – **for the bad guys**. 2016 was so big that cybercriminals had trouble selling medical records on the dark web due to market saturation! We knew it was going to be an exceptional year for the bad guys, but no one could have predicted just how much the cybercrime economy would grow over such a short period of time.

So what's next? Is 2017 totally doomed? It seems that with every new breach comes a new fix, and with every new fix comes a new cybercrime innovation. It's just like a military build-up or arms race, except this time the battlefield is the internet.

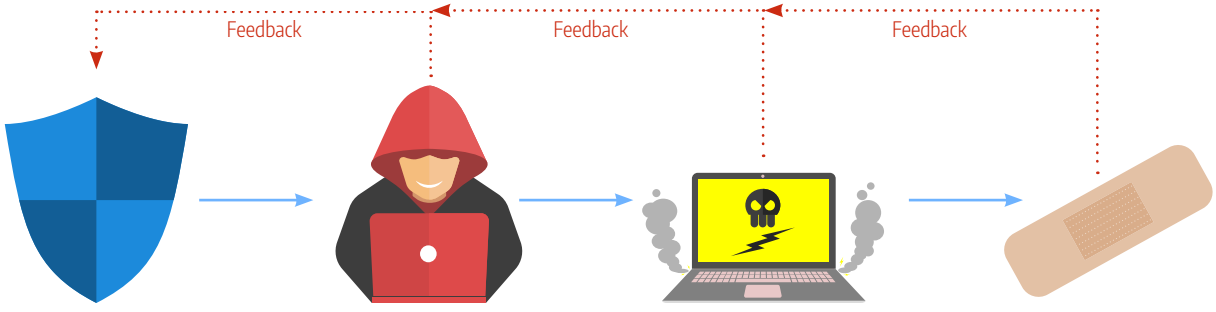
Are planes, trains and automobiles next? Of course they are! Tesla got hacked (again) in November 2016. What about internet-connected appliances and gadgets, like refrigerators, coffee makers and thermostats? Is the future of technology anything more than a future of unsecured devices? IoT developers have largely *not* paid sufficient attention to security or made it a priority, even though all of these devices WILL touch the internet, as well as our personal, professional and mobile lives.

Cyber threats are not going away. Most experts think **the Security of Things will get worse before it gets better**. Tech companies will continue to release products rife with security flaws, errors or misconfigurations. Cybercriminals will continue to discover new ways to find and steal data and to compromise organizations. Information security is an endless circle, a loop if you will. *(See image below.)*

But there is hope. And that hope is *you*. It's me. It's your coworkers and family members. It's all of us!

Being proactive with security efforts is the only way we'll strengthen our position in the constant "tug-of-war" with cybercriminals. We can't predict what the next new wave of cyber threats will be in 2017, but we can rely on security fundamentals with a proven success rate to minimize their effect. The simplest things work best: stay alert to your physical, personal and cyber environment; have prudent situational awareness; update security preferences for every device you own; develop strong, unique passphrases; and, as always, think before clicking.

If everyone does their part, maybe we'll have a different – more secure – conversation at this same time next year.



Good security comes from timely response. Report security incidents immediately!

2016 TIMELINE OF CYBERATTACKS

JANUARY

CEO fraud hits Crelan, a major bank in Belgium, resulting in a loss of over 70 million euros (78 million USD).

FEBRUARY

The US Internal Revenue Service gets infected with malware; electronic tax-return credentials for 101,000 social security numbers stolen.

MARCH

Verizon Enterprise Solutions hacked; database of over 1.5 million customers posted on an underground cybercrime forum.

APRIL

Details of nearly 50 million Turkish citizens posted online with download links available to anyone interested.

MAY

Anonymous launches a 30-day campaign known as Operation Icarus and takes down several central banks worldwide via DDoS attacks.

JUNE

Badoo, a UK dating-focused social networking service gets hacked, exposing over 127 million accounts.

JULY

Taiwanese banks suspend ATMs after cybercriminals use malware to steal millions. Experts believe the thieves were able to connect to the ATMs using smart phones.

AUGUST

Bitfinex, a Hong Kong-based digital currency exchange platform, gets hacked; cybercriminals steal $65m (£48m, €57m) in Bitcoin. The value of bitcoin plummets as a result.

SEPTEMBER

Rambler.ru, a Russian internet portal and email provider, hacked; 98 million accounts leaked.

OCTOBER

Modern Business Solutions hacked; 58 million customers' data leaked, including full names, emails and postal addresses.

NOVEMBER

AdultFriendFinder.com hacked for the second time in two years. Over 400 million users' personal data stolen.

DECEMBER

Dailymotion, one of the most popular video-sharing sites on the web, admits hack exposed millions of accounts. Over 85.2 million unique email addresses and usernames stolen.

CEO Fraud: Unlike standard phishing attempts, cybercriminals generally don't use malware to victimize CEOs. Instead, they'll collect data related to their target and spoof the email of a legitimate institution or someone the victim often does business with to trick them into wiring money to the attacker.

DDoS: Short for distributed denial-of-service, DDoS attacks are carried out by compromised internet-connected devices, such as DVRs and gaming systems. The attacker gains control of these devices—without the owner knowing—and points them at a specific server. They then flood the server with more information than it can handle, causing it to crash. This is how several major websites were knocked offline in late October.

Do you know what all of these security incidents have in common? They all involved people. Not just people getting hacked, but people making mistakes. Someone, somewhere, clicked on something they shouldn't have or otherwise failed to follow the appropriate steps to enhance security. It happens. *Here are five things to do if your account is associated with a data breach.*

1. **Update all of your passwords immediately. This is a tedious exercise, but you can bet cybercriminals are going to use those cracked credentials to gain access to other accounts. Good password managers can make this task less daunting. This is non-optional.**
2. Place a fraud alert on your credit report. There are several credit bureaus worldwide. Here's a resource to get you started: https://en.wikipedia.org/wiki/Credit_bureau
3. **Inform your banks and financial institutions immediately. Regardless if it's a data breach or ID theft, chances are your banks will want to update your account with new numbers, credit cards and debit cards. Yes, it's a pain, but the alternative is much worse.**
4. Be aware of related attacks! You are now on "the list." If one of your accounts was compromised, you can reasonably anticipate a string of phishing attempts. Always verify the legitimacy of an email, and think before you click.
5. **Monitor your credit reports. The aftermath of a data breach often lasts for a while. It's best to check your credit report at least monthly to keep an eye out for fraudulent activity.**

Good security comes from timely response. Report security incidents immediately!

Cybersecurity Ventures, a research & market intelligence firm, projects that nearly 1 trillion dollars (930 billion euros) will be spent globally on cybersecurity from 2017 to 2021. But the important thing to remember is that combating cybercrime also requires massive human effort to be effective. Security is not only a financial issue. To adequately defend our cyber-lives, we ALL need to be strong human firewalls and not passively rely on cybersecurity technology.

2017 THE YEAR WE FIGHT BACK!

TOP FIVE Security Fundamentals to Combat Cybercrime

ONE: **Implement a strong, unique passphrase for every account.** We're done with passwords—even those that are made up of nonsense to appear uncrackable. Passphrases are a far superior security mechanism. Take some time to update your passwords to passphrases. This is a lot easier to accomplish with a password manager, which is easy to use, inexpensive, and most importantly, secure.

TWO: **Change your behavior.** Too often we hear the term "common sense" thrown around as if it's a standard, objective part of information security. Yes, we encourage the use of common sense, but it's subjective. If common sense had a history of success, cybercriminals would be struggling. That's not the case. Instead we need to change our behavior.

THREE: **Follow policy.** Rules and regulations within our organization exist for a reason. Without policies, we can't operate our business successfully; the confidentiality, integrity and accessibility of sensitive data would be vulnerable. Please familiarize yourself with our policies and guidelines. When in doubt, ask!

FOUR: **Join the conversation.** We live in an age of overwhelming information. As such, communication is one of the most important skills any of us can use, learn and improve. The more we discuss, the more we'll know, and the more secure we'll be.

FIVE: **Lead by example.** Not everyone in our life values information security the way we do. That's why we all must set a good example and spread the word to our friends and families. Leading by example is a proactive approach that undermines cybercriminals.

Common Sense Security

Applying What You Know to What You Do

Common sense is important. But human behavior is what cybercriminals target. Social engineers exploit poor behavior and leverage psychological responses against victims. It's how they get you to click. Here are five ways we can convert our common sense to a change in behavior that will make us strong cyber-aware citizens.

Common Sense >> I should use a strong and unique password to protect each of my accounts.

Behavior Change >> I will use a strong passphrase that's easy to remember but hard to guess, turn on two factor authentication whenever it's available, and utilize a password manager so I only have to remember one master password.

Common Sense >> I should always follow policy at work.

Behavior Change >> I will always follow policy at work and will set up a similar home and mobile policies for personal and family use.

Common Sense >> I should make my employees take security awareness training.

Behavior Change >> I will learn how to become a human firewall and lead by example. I will empower my staff to learn by doing instead of just giving them a set of rules to follow. (Though this is aimed at upper management, the fundamental message is about a culture of security awareness, which all of us should participate in!)

Common Sense >> I should install a comprehensive anti-virus/anti-malware program so my computer doesn't get infected.

Behavior Change >> I will install anti-malware on all my devices—not just computers, but tablets and phones too.

Common Sense >> I should always wear my badge before entering a controlled access building at work.

Behavior Change >> I will always report or politely challenge anyone not wearing a badge in a controlled access area to prevent any potential social engineering attacks in the future.

Good security comes from timely response. Report security incidents immediately!

WHAT DOES THE FUTURE HOLD?

The Future of Ransomware

Meet Locky. If awards were given out to cybercriminals, Locky would sweep as the most valuable malware of 2016. According to Malwarebytes, the Locky family of ransomware spread to **18 different countries on the first day of its detection (February 2016)** with more than 100,000 infections each day. By day three it was in 84 different countries, and in over 100 by the end of its first week. Here we are, nearly a year later, and it is still being detected in nearly 200 countries, including Antarctica, making it the only known family of ransomware to hit every continent.

Clearly, this is a global phenomenon and a trend that is likely to be reproduced in 2017. What will be different, if anything? Locky will eventually be replaced with malware that is harder, better, faster, stronger. **Security experts fear new versions of ransomware will act as cryptoworms, which means once the malware infects one machine or device, it will self-propagate and spread to every device on the same network.** The cost of ransoms will likely rise in coming years as cybercriminals pressure organizations by slowly releasing data to the public and/or slowly deleting local backups until payments have processed.

Their targets? **Most agree that the Internet of Things will be next, with DVRs, security cameras, gaming systems and routers at the top of the list. And, of course, your smart devices like phones, tablets and watches.** Others fear critical infrastructure like power grids and water treatment systems will see a wave of attacks globally.

But regardless of technology, the consensus is that ransomware will maintain its dominance with the same methods it did in 2016: via social engineering. That's why it's up to all of us to maintain a high standard of cyber awareness. Expect to see a rise in phishing attempts during the coming year. Train yourself to carefully read every email and verify sources. Follow company policy and know how to report suspicious activity. Update your usernames and passwords so they are unique across every account. **Let's put cybercriminals out of business and make Human Firewalls the MVP of 2017!**

THE FUTURE OF CYBERCRIME

Cybercrime is projected to cost businesses over 2 trillion dollars USD (1.8 trillion EUR) annually by 2019—a fourfold increase from 2015.

(source https://www.checkmarx.com/2016/05/25/cyber-crime-statistics-infographic/)

HOW CAN I HELP OUR ORGANIZATION FIGHT BACK AGAINST CYBERCRIME THIS YEAR?

Follow policy! Our organization's policies don't exist because we like rules but rather to protect the sensitive data of our clients, coworkers and consumers. If you're not sure what our policies are, please ask!

TO POLICY AND BEYOND!

Three things you can do that go above and beyond company policies: *(After you learn ours, of course!)*

Lock your computer when you leave your work area. Even if you get up to stretch for a couple of minutes, be sure to log out so no one can access your computer for any reason.

Keep a clean work environment. It's easy to lose thumb drives, badges and sensitive documents if your desk is a mess. Prevent that from happening by keeping things orderly! Cleanliness is just good security.

Report potential security incidents immediately. Even if you're not sure if it qualifies as a security incident, tell someone! Things like locked doors being left open or unidentified packages left in the lobby can lead to a breach in security and need to be reported.

Good security comes from timely response. Report security incidents immediately!

HEADLINE NEWS

Police ask for Amazon Echo data to help solve murder case.

Investigators of a murder in Bentonville, Arkansas have requested access to audio that may have been recorded on an Amazon Echo. The electronic personal assistant records and stores audio in the cloud when it hears a "wake word" (such as 'Alexa' or 'Amazon'). Police say the Echo was in the kitchen of the victim's home and could lead to clues in the quest for justice.

The request has raised new questions regarding electronic privacy, similar to when the FBI ordered Apple to unlock an iPhone in the 2015 San Bernardino attack that killed 14 people. Amazon has so far denied the investigators' request stating that it "objects to overbroad or otherwise inappropriate demands." In what's clearly a gray area, more and more cases like these are bound to arise as more and more of our private information is stored electronically. To read more, visit http://secaware.co/2iKLfC5

Cybercriminals steal millions from Russian central bank.

The Bank of Russia confirmed cybercriminals were able to steal 2 billion rubles—the equivalent of $31 million—in 2016. Some of the initial attacks were thwarted and funds were redistributed, but thieves were still able to successfully compromise the bank's security. Officials say the attackers used spoofed credentials for one of the bank's customers to gain access.

The specifics of when the heists occurred have not been reported. Nor is clear who is behind the attacks. According to CNN, the attacks are similar to a string of bank heists that targeted the worldwide financial system. The key difference in this case is the plot also involved social media disinformation. The FSB—Russia's top law enforcement agency—said the attackers planned to spread fake news about Russian banks questioning their financial stability. To read more, visit http://secaware.co/2hZAPuA

BBC

BBC News • Dec 1
TalkTalk and Post Office routers targeted in cyberattack. http://secaware.co/2hRBvGU

IBT

International Business Times • Dec 15
Cybercriminals write code to hijack routers and insert malicious ads. http://secaware.co/2hQXKrS

SP

SOFTPEDIA • Dec 15
Russian Visa website hack exposes data of thousands of users.
http://secaware.co/2hRI6S3

TM

Trend Micro • Dec 19
Fake apps take advantage of Super Mario Run release. http://secaware.co/2hR1eui

COM

Cult of Mac • Dec 22
Russia wants Apple to unlock Turkish assassin's iPhone. http://secaware.co/2iEhlNW

UPI

United Press International • Jan 3
North Korea cybercriminals launch attack on South Korea after New Year's Day.
http://secaware.co/2hRJiEW

BBC

BBC News • Jan 3
Data breach exposes US army doctor details.
http://secaware.co/2ilPjmV

THN

The Hacker News • Jan 4
Bitcoin price rises to the highest level in three years. http://secaware.co/2j58lk3

Good security comes from timely response. Report security incidents immediately!