TECHVERA

The Business Guide to Cybersecurity

Computer Security

Table of Contents

INTRODUCTION

Cyber attack threats seem to grow greater every day. News of widespread hacks, leaked information, and attacks that bring down entire businesses can leave anybody feeling vulnerable. It is especially important as a company dealing with personal client and team information to be as aware and secure as possible against threats. **It is much more effective to prevent an attack than to deal with the aftermath.** Most people realize the importance of good cybersecurity, but few truly act upon it. To give you a better idea of how imperative it is to be prepared and protected, check out these cyber attack stats from Symantec, the creators of Norton Antivirus:

- **A new zero-day vulnerability is discovered each week** - zero-day attacks involve hackers finding a flaw in a piece of software that allows them to infect its users, before the software maker can fix it. "In 2015, the number of zero-day vulnerabilities discovered more than doubled to 54, a 125 percent increase from the year before".

- **Half a billion personal records stolen or lost** - "In 2015, we saw a record-setting total of nine mega-breaches, and the reported number of exposed identities jumped to 429 million. But this number hides a bigger story. In 2015, more companies chose not to reveal the full extent of their data breaches. A conservative estimate of unreported breaches pushes the number of records lost to more than half a billion."

- **Vulnerabilities found in 3/4 of websites** - "There were over one million web attacks against people each day in 2015. Cybercriminals continue to take advantage of vulnerabilities in legitimate websites to infect users, because website administrators fail to secure their websites. Nearly 75 percent of all legitimate websites have unpatched vulnerabilities, putting us all at risk."

- **Ransomware increased 35 percent** - "An extremely profitable type of attack, ransomware will continue to ensnare PC users and expand to any network-connected device that can be held hostage for a profit. In 2015, ransomware found new targets in smart phones, Mac, and Linux systems."

- **Symantec alone blocked 100 million fake technical support scams in 2015** - "Fake technical support scams have evolved from cold-calling unsuspecting victims to the attacker fooling victims into calling them directly. Attackers trick people with pop-up error alerts, thus steering the victim to an 800 number where a "tech support rep" attempts to sell the victim worthless services."

Security threats come in many forms - malware, ransomware, phishing, denial of service, Trojans, and more. In this eBook, we'll cover the different types of attacks you are most likely to face and how you can prevent them hurting your business - or recover after an incident.

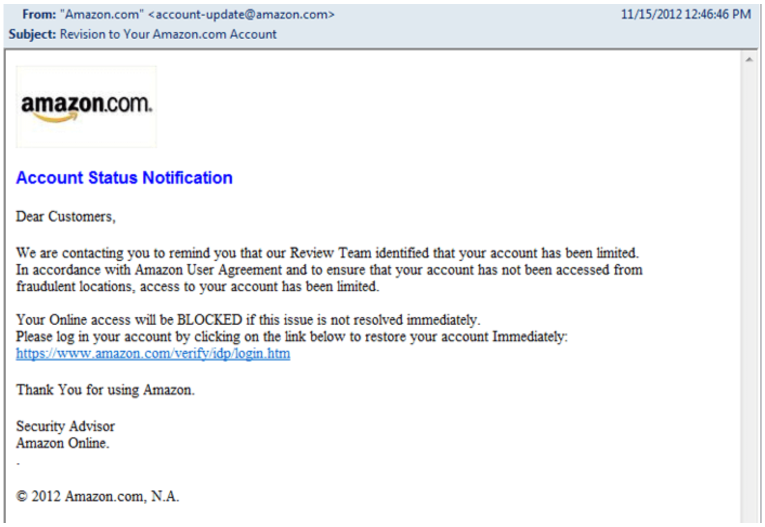
PART ONE - TYPES OF SECURITY THREATS & HOW TO AVOID THEM

1) Phishing

Definition: "A scam by which an e-mail user is duped into revealing personal or confidential information which the scammer can use illicitly" (Merriam-Webster)

These attacks mainly pose as requests to verify information, and the scammer attempts to make them look as legitimate as possible to confuse the victim. These emails may appear to come from an institution you use that holds valuable financial information such as your bank, PayPal, online subscriptions, a mailing service, or the IRS. The fradulent emails will tell you that your online information needs to be verified, is out of date and needs to be updated, that you have a message, or that something is wrong and you need to log into your account to fix it. Clicking on the link they provide will take you to a page that looks like the login for the service, but is actually a fake page set up by the scammer to trick you into entering your personal information that they will then receive and use. These are an even bigger threat for businesses versus home users as scammers using these attacks have been known to send emails posing as a company employee, tricking other employees into following a link and giving up organizational login information.

Examples of phishing emails



From: "Amazon.com" <account-update@amazon.com> 11/15/2012 12:46:46 PM
Subject: Revision to Your Amazon.com Account

Account Status Notification

Dear Customers,

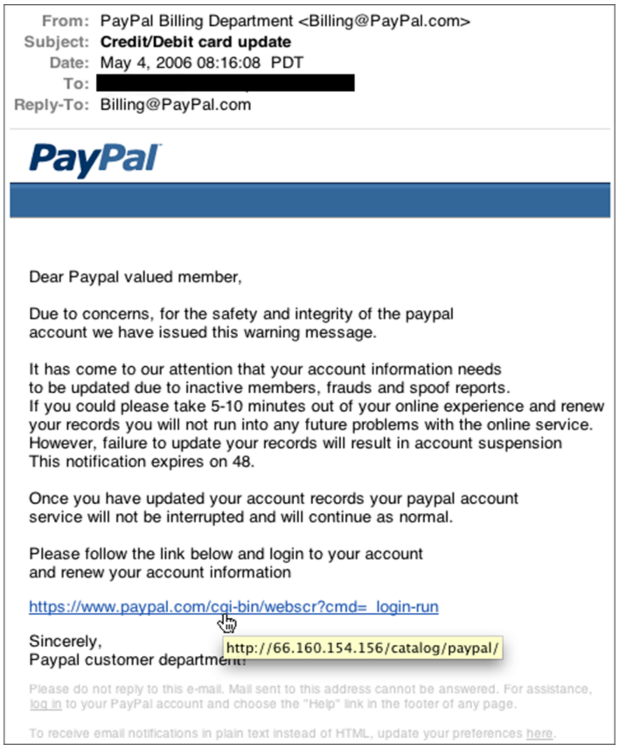
We are contacting you to remind you that our Review Team identified that your account has been limited. In accordance with Amazon User Agreement and to ensure that your account has not been accessed from fraudulent locations, access to your account has been limited.

Your Online access will be BLOCKED if this issue is not resolved immediately.
Please log in your account by clicking on the link below to restore your account Immediately:
https://www.amazon.com/verify/idp/login.htm

Thank You for using Amazon.

Security Advisor
Amazon Online.
.

© 2012 Amazon.com, N.A.



From: PayPal Billing Department <Billing@PayPal.com>
Subject: **Credit/Debit card update**
Date: May 4, 2006 08:16:08 PDT
To: [redacted]
Reply-To: Billing@PayPal.com

Dear Paypal valued member,

Due to concerns, for the safety and integrity of the paypal account we have issued this warning message.

It has come to our attention that your account information needs to be updated due to inactive members, frauds and spoof reports.
If you could please take 5-10 minutes out of your online experience and renew your records you will not run into any future problems with the online service.
However, failure to update your records will result in account suspension
This notification expires on 48.

Once you have updated your account records your paypal account service will not be interrupted and will continue as normal.

Please follow the link below and login to your account and renew your account information

https://www.paypal.com/cgi-bin/webscr?cmd=_login-run

http://66.160.154.156/catalog/paypal/

Sincerely,
Paypal customer department

Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, log in to your PayPal account and choose the "Help" link in the footer of any page.

To receive email notifications in plain text instead of HTML, update your preferences here.

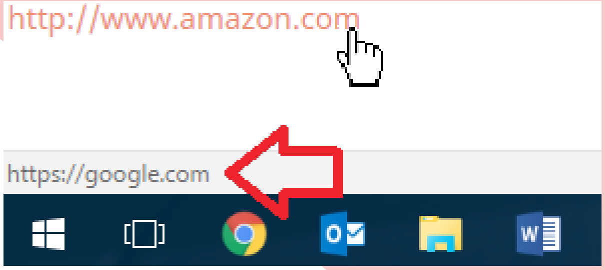
How to spot and avoid

While many of the phishing emails you'll receive are clearly fakes littered with spelling and grammatical errors, obviously false email addresses, and nonsensical instructions, these attacks are becoming more sophisticated every day. Many are difficult to distinguish as fake. Here are a few techniques they use and how to spot them:

Fake links

Hyperlinks can look like they will lead you to a legitimate site, but they can actually go wherever the creator wants them to. For example, you would expect clicking this link: http://www.amazon.com would take you to Amazon, right? However I've told the code powering it to direct the clicker to Google instead. The text shown and the actual link destination don't have to match whatsoever. This is how scammers trick people into thinking they're going to something like their bank website when in fact they're going to that scammer's fake bank login page.

So how can you tell where a link will take you? By hovering your mouse cursor over the link without clicking, a bar will pop up in the lower left corner of your screen that shows where you will go when you click. Here's an example with that same Amazon-Google link trick:



Email address spoofing

Spoofing really just means faking, and it's the term for when scammers mask their sending address to make it look like the email is coming from someone else - a trusted organization, family member, or friend for instance to improve the chance that you'll click on their link. Unfortunately there is really no easy way to determine when this is happening just by looking at the address. Best practice is to not click links in these emails unless you were expecting them, and contact the sender by phone or in person when in doubt. People whose email accounts have been hacked may also send out mass emails with bogus links.

To click or not to click?

It's best to treat emails with links like emails with attachments. If you are expecting the email - say you just ordered a package from Amazon and receive an email with your tracking code - go for it. If the email is out of the ordinary, unexpected, asks you to confirm/enter financial or personal information, or looks "phishy" in any way, it's best to err on the side of caution. Businesses that handle financial and personal information have strict rules against ever asking you for information over email. You can always call to confirm the information from the email, or instead manually log into the website account in question without following the provided link.

2) Security exploit

Definition: "An unintended and unpatched flaw in software code that exposes it to potential exploitation by hackers or malicious software code such as viruses, worms, Trojan horses and other forms of malware" (Webopedia)

When a pop-up from software you use comes up on screen asking you to update it, do you? Do you immediately close that annoying Windows Update prompt? Many people do - and this is what leads to security exploits! Software is certainly not perfect on release day, and the developers are constantly fixing holes and security flaws. These solutions are released in patches and updates. If you are ignoring these updates you are opening yourself up to a wealth of infections or even people spying on your activity.

These aren't just limited to computers either! Consider these...

Examples of real-life exploits

HP Printers

In January 2013, a ViaForensics researcher Sebastian Guerrero discovered vulnerabilities in HP's JetDirect technology that could be used to both crash the hardware or gain access to previously printed documents. You could imagine how bad that situation could be for a business that prints sensitive or confidential information. Andrew Howard, an app developer, followed this discovery with a blog post outlining how easy it was to find tens of thousands of Web-accessible HP printers just waiting for hackers to take advantage of security holes.

Cisco Videoconferencing Software

Videoconferencing software is popular in many business environments, but the ability to watch and listen in from this software can be a hacker's dream. This happened in 2010 with Cisco's Unified Videoconferencing products, and granted the attacker full access to the hardware as well as any connected networks. In January 2012, security researchers found around 150,000 videoconferencing systems configured to answer calls automatically, which means anyone with access could tap into the video and microphone at any time. Luckily Cisco quickly patched this flaw as soon as it was found.

Adobe Flash Player

Unfortunately Adobe Flash is known for being a hotbed of exploits and security flaws. One of the more recent vulnerabilities came to light in January 2016, and allowed hackers to remotely execute code and take control of victims' computer systems. When its emergency patch was released, it came only two weeks after Microsoft's October patch fixed nine other critical vulnerabilities in Flash.

Ensure your software is on a patch and update schedule, and don't ignore warning boxes!

3) Malware

Definition: "Malware, short for malicious software, is any software used to disrupt computer operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising" (Wikipedia)

Malware is actually a blanket term and covers viruses, Trojans, worms, spyware, adware, scareware, and ransomware. These are a lot of different terms, so let's go over the traits and warning signs of each different type.

Virus

A program or piece of code loaded onto your computer that attaches itself to a program or file, enabling it to spread and leaving infections as it travels - just like a human virus. Some are mild and simply annoy the user, and others are far more dangerous - corrupting files, data, and even hardware. Viruses can run in the background and use up resources like memory very quickly, which is why infected machines tend to be very slow and difficult to use. Viruses cannot spread without human action, such as opening an infected file.

Trojan

Malware disguised as legitimate software - you can see why it was named after the famous Trojan horse! Trojans can delete, block, modify, and copy data, and disrupt the performance of infected systems. Unlike viruses and worms, Trojans do not replicate or infect other files.

Worm

Similar to viruses, worms are unique in their capability to travel without human interaction. After replicating itself on your system, it could send not only the one but hundreds of copies to say, everyone in your email contact list. The same thing happens to those users, and the worm quickly spreads, likely without anyone being the wiser. Because of its ability to grow and spread it can consume huge amounts of system memory or network bandwidth and shut down Web and network servers, or cause computers to stop responding.

Spyware

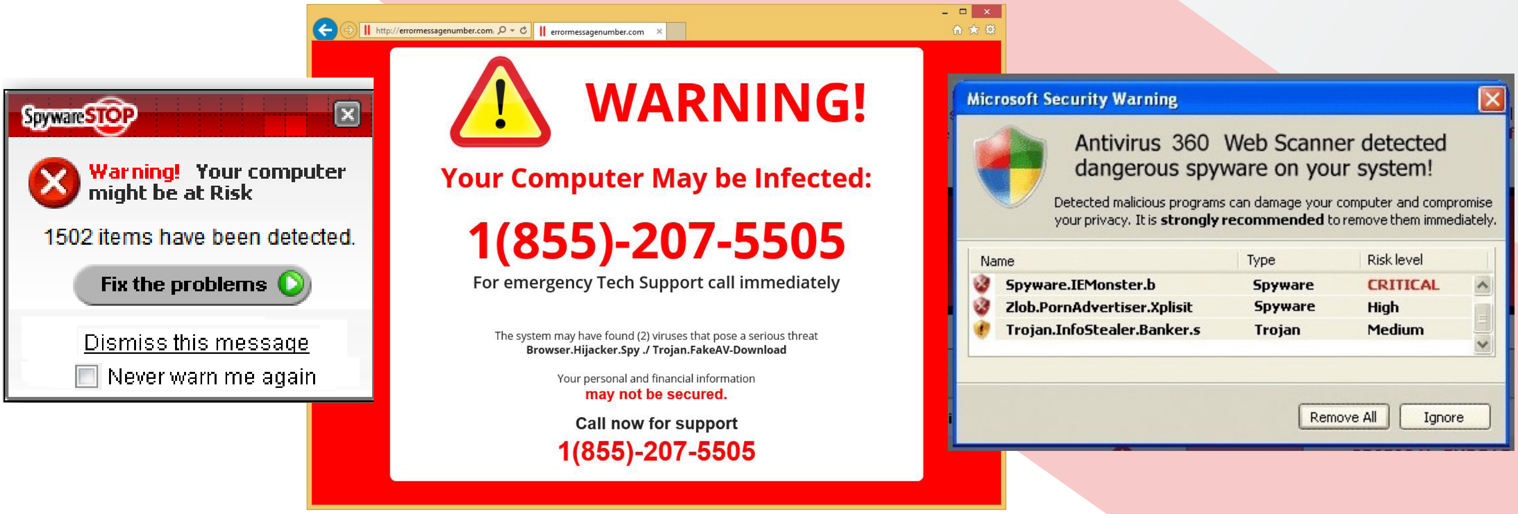
Simple enough to remember - software that spies on you. These programs will covertly gather and transmit information about your keystrokes, Internet browsing habits, device usage, and personal data back to their creators. The tracking software that many companies use to monitor employees' usage can be considered a form of non-malicious spyware. It is only truly considered spyware when the user is not made aware that they are being tracked. This malware can be hard to detect, generally the only noticeable signs will be a decrease in performance, connection speed, and data usage and battery life when on mobile devices.

Adware

Arguably the least malicious but most annoying, adware causes your computer to display advertising banners and popups during use. Adware is commonly bundled with free software to help offset the costs for the developers. However much adware also falls into spyware classification by tracking the user's habits and sending data to 3rd parties for additional advertisement.

Scareware

The 'scare' in the name comes from this malware's habit of attempting to frighten you into installing malicious, deceitful software. Usually you'll receive a popup or error message using bold, flashy graphics and words to attempt to convince you that your computer is severly infected and you must install the advertised program to fix the issues. Downloading the phony fix software can install even more malware on your machine, trick you into giving them your money, or even lock down your computer/encrypt your files to make them unuseable (see ransomware).



Warning! Your computer might be at Risk

1502 items have been detected.

WARNING!

Your Computer May be Infected:

1(855)-207-5505

For emergency Tech Support call immediately

The system may have found (2) viruses that pose a serious threat
Browser.Hijacker.Spy ./ Trojan.FakeAV-Download

Your personal and financial information
may not be secured.

Call now for support
1(855)-207-5505

Antivirus 360 Web Scanner detected dangerous spyware on your system!

Detected malicious programs can damage your computer and compromise your privacy. It is **strongly recommended** to remove them immediately.

Name	Type	Risk level
Spyware.IEMonster.b	Spyware	CRITICAL
Zlob.PornAdvertiser.Xplisit	Spyware	High
Trojan.InfoStealer.Banker.s	Trojan	Medium

Ransomware

Ransomware has been everywhere lately, with more users getting infected than ever before. It literally holds your entire system and/or files for ransom. Lockscreen ransomware will completely prevent you from accessing your computer, and demand a payment to unlock it. Encryption ransomware will encrypt all of your computer's data, making it unuseable and unreadable without the decryption key - which only the malware creator has. They will also demand payment to allow you to get your files back, otherwise you'll lose that data forever. Many forms of ransomware have been cracked and repair centers can now fix them without your needing to pay, but there are new ones created all the time. The best way to avoid losing access to your files or computer is to always maintain current backups. Should your computer become infected, reloading the operating system and restoring your files will get you back to 100% without losing hundreds of dollars.

4) Denial-of-service (DoS)

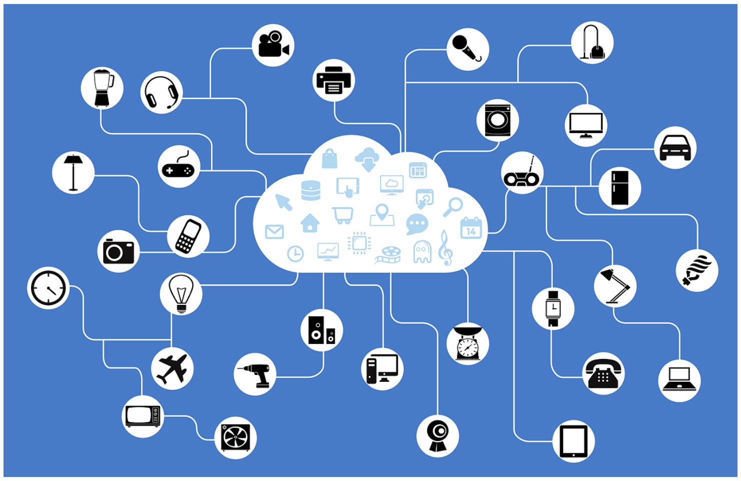
Definition: "A DoS attack focuses on disrupting the service to a network. Attackers send high volumes of data or traffic through the network (i.e. making lots of connection requests), until the network becomes overloaded and can no longer function." (intuit)

We mainly hear about these in the news as DDoS attacks, which stands for distributed-denial-of-service. The attacker employs multiple computers or devices that he has installed a piece of malware on that will aid in the attack. The true users of the devices will likely not even realize that they are part of the attack! Most services have a maximum amount of traffic or bandwidth they can reasonably handle at once. The attacker knows this and overloads their system with so many requests that the website or service goes past its limit and stops functioning.

Why would someone perform a denial-of-service attack?

What's the benefit other than some hacker's personal satisfaction, right? Many large-scale attacks of this nature have been used to protest governments, terrorist groups, people, or events by shutting down their website and ability to communicate with their followers.

In October 2016, we just witnessed a large DDoS attack on a DNS (doman name server) company called Dyn, which caused a number of popular sites to go down - Reddit, Twitter, Spotify, SoundCloud, and Shopify among them. An estimated 100,000 infected devices aided in the attack. The infected included a number of Internet of Things devices like security cameras and smart electronics which are notoriously insecure and easy to compromise. Dyn has not discovered why the attacks were happening as they received no message from the attackers. However they believe someone is currently testing the security capabilities of companies that provide critical internet service - a scary prospect.



Should you be worried?

Unless you're a very large company, it's unlikely that you'll ever be hit with a DoS attack. However your website or network could be affected if another organization on your network or hosting company falls victim.

The best way to mitigate one of these attacks is to keep your system and applications current with regular updates and patches, and monitor your online security and data flow to identify any unusual traffic.

If you or your business uses internet-connected or IoT devices, it's also important to ensure they are secure so they don't become infected and aid in an attack like this. It's become popular for attackers to infect these weak devices to help their cause.

PART TWO - HOW TO HANDLE A CYBER ATTACK

Sadly, no security plan is 100% foolproof and it's impossible to completely prevent cyber attacks and infections. "More than 80 percent of U.S. companies have been successfully hacked, according to a Duke University/CFO Magazine Global Business Outlook Survey" released in 2015. Smaller companies are even more vulnerable than large ones due to more limited budgets and staff, "with 85 percent saying their information systems had been broken into. About 60 percent of larger companies reported successful hacks". (CBSnews.com)

The more precautions and resources you can dedicate to cybersecurity, the less likely a severe breach will ever occur. But it's always best to have a game plan in case something does make it through. You can improve response times and mitigate damage by knowing the steps to take.

Before

Education is the best prevention

In addition to securing your company as much as possible through regularly updated software, comprehensive virus/malware protection, and network security, your staff must be aware of best security practices and policies. Educate your team on the different ways attackers try to get in, what common tactics look like, and who to contact should they expect a current or potential infection/breach. **52 percent of security breaches in businesses are caused by human error.**

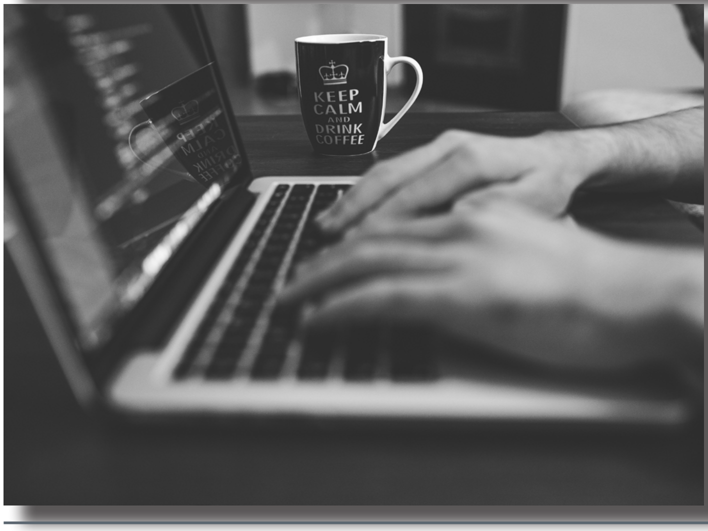
Consider making security policy and education training part of every new employee orientation program, and hold weekly or monthly meetings for the staff to get up-to-date on new threats and methods being used by attackers.

For a good preventative starting point, check out our guide on how to spot, avoid, and remove malware/viruses

Random security audits are used by many companies to ensure everyone is following procedures.

There are also technologies available to "detect whether sensitive data is being sent over email or copied to a USB stick. A determined employee will find ways around, but this type of monitoring and detection can help minimize innocent mistakes." (SC Media) These are called data loss prevention (DLP) solutions.

Most importantly, have a plan! Meet with your board members, investors, lawyers, IT team, and staff. Ensure that should something happen, everyone knows their role and what steps will be taken to protect the company and mitigate damage.



During

Make sure everyone knows where to go when it's go time

An incident response (IR) team is essential to your organization. This should include all relevant stakeholders, technical staff, board members, your legal team, and anyone else who will need to help the company recover from an attack. When things hit the fan, these people will know exactly what needs to be done to minimize damage and get operations back to 100%.

The rest of your staff needs to know their roles during an attack as well. Many people have the urge to ignore or cover up possible signs of an infection or hack, either not thinking they're in danger or not wanting to admit they may have made a mistake. **Ensure your team knows that they will never be retaliated against for bringing a possible situation to light.** Whether they tell you or not, what's happened has happened and ignoring/fearing it will only make things worse for everyone!

People also have a natural urge to try and stop attacks themselves - often this manifests in immediately powering down their computer to try and cut off the hacker. While this does effectively keep someone from using your computer any further, it wipes evidence and data away, not to mention tips off the hacker that the company is onto him. There have been numerous instances where this very situation happened within a company and the hacker simply hid - sometimes for months at a time - until things died down before launching yet another, even more advanced attack. Teams need to give the IT and IR groups all the data and opportunity they can to solve the problem correctly.

After

Recover and learn

Notify authorities and clients who may be affected. If there is even a remote possibility that your customers' financial or personal information is compromised, tell them as soon as possible. They will find out eventually, and as we've learned with the recent influx of large data breaches, the longer you wait the more incensed your customers will be. The sooner they know, the sooner they can take steps to prevent negative consequences and you will garner goodwill for your quick communications. Letting law enforcement know about the attack can give them data to help prevent similar ones from hitting other businesses.

Once you're in recovery mode, **continue to monitor your network(s) and systems**. Attackers can covertly install backdoors that will allow easy access for their next attack. Have your IT team keep a very close eye on your technology for at least the next month (and don't forget about all those devices your staff has - phones, tablets, and other WiFi-connected electronics). Do regular security checks.

This is a learning opportunity for your company! While no cybersecurity plan is 100% foolproof, you've just gained valuable insight into the weak points of yours. Bolster your security efforts, patch the holes the attacker used, and take this as a chance to improve.

TECHVERA

Need security help for your business?

Sometimes you need help from the experts - we've got you covered. Fill out our contact form using the button below, or give us a call to set up a free consultation.

Schedule a Consultation

Want to learn even more? Our blog is full of security tips and news on the latest threat landscapes.