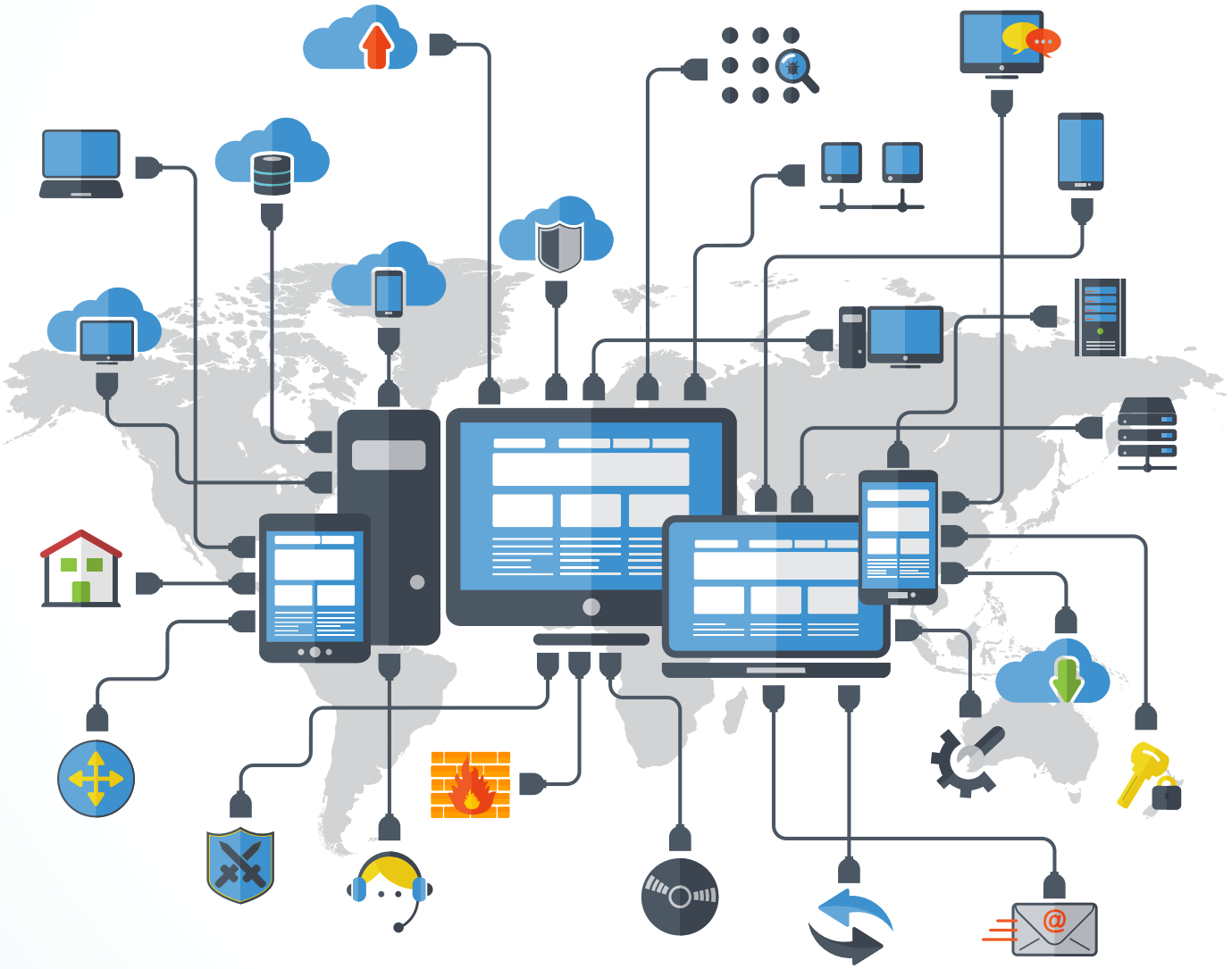
Cybersecurity Business Training

A Guide to Preventing Business Cybercrime



ANDERSON TECHNOLOGIES

A Handbook by Anderson Technologies, a St. Louis IT Company
info@andersontech.com | https://andersontech.com | 314.394.3001

Cybercrime Is on the Rise

Cybercrime is the fastest-growing threat to businesses and individuals in the United States. Perpetrators use nefarious tactics and tools like malware, viruses, spyware, bots, phishing, and spear phishing to perform a host of crimes, including fraud and theft of valuable data like credit card numbers, passwords, and personal health information.

In 2018, more than 5.3 billion personal records were exposed or stolen in known security breaches, both malicious and accidental. In 2019, that figure jumped to 15.1 billion personal records compromised.[1]

Most cybercrime is preventable, but even if you are doing everything right, it takes just one wrong click to breach your digital "fortress." That's why it is so important that all members of a business team understand digital best practices and how to protect themselves from cybercrime.

In this handbook, you will learn about:

- The state of small business cybercrime
- Email red flags, including examples of real spear phishing emails
- Internet safety tips and warning signs
- What to do if you've clicked or downloaded something you shouldn't have

Cyber Threats Against Small Businesses Are Growing

Over the last few years, cybercriminals have started targeting small businesses more frequently. According to Datto, one in five small- and medium-sized businesses reported being victim to a ransomware attack.[2] The average cost of downtime due to a ransomware attack in 2019 was $141,000, up from $46,800 the previous year.[3]

Part of the reason small businesses are increasingly targeted is because many do not take the necessary steps to stay secure. This makes them easy targets.

To ensure digital safety, every small business must:

1. Install a hardware firewall that is continually monitored and patched.

2. Install anti-virus and anti-malware software on all devices and keep them updated.

3. Back up all business-critical files regularly and test their ability to be restored.

4. Regularly update all devices with the latest operating systems and third-party application patches.

5. Adopt a policy of least trust. Share data only with those who need it.

6. Educate employees about safe digital practices.

The last one is important. Even if you are completing steps one through five diligently, it only takes a single bad decision by one employee to throw all your hard work out the window.

Cybercriminals Are More Sophisticated

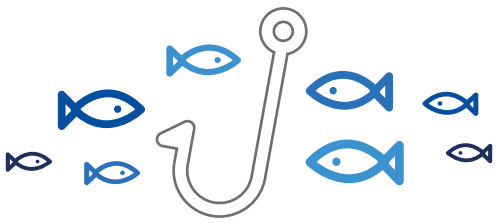
Phishing emails are a cybercrime tactic in which the sender tries to elicit personal information from the recipient. They are sent to a wide audience and are often recognizable as fraudulent because of the content, strange spelling errors, or unnatural syntax. For example, you may have received an email from a "prince" in some far away country who is eager to give you millions. Most employees are aware that such emails are hoaxes.

Unfortunately, the bad guys have gotten better. Phishing has evolved into spear phishing, a similar but more sophisticated con in which a criminal targets a specific person and crafts a believable email based on personal information obtained about the recipient.

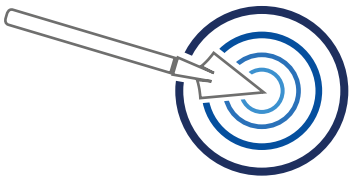
Spear phishing emails often appear to come from a colleague, friend, family member, or business associate. They are usually well designed and written convincingly enough to seem completely legitimate.

How Do Hackers Get My Info?

Even if you've done everything right, cybercriminals could still glean enough information to target you via a phishing scam. They may have hacked a site with your contact information, such as an online shopping company or an email provider, or mined public imformation availble on your social media accounts. Your data can even be compromised by companies you have never interacted with. In November 2019, a server with more than **1.2 billion personal records** was found open to the internet on an unprotected server. The owner of the server is unknown, but it's believed to be a data enrichment company.[4] This is the type of incident that gives cybercriminals the information they need for more convincing scams.

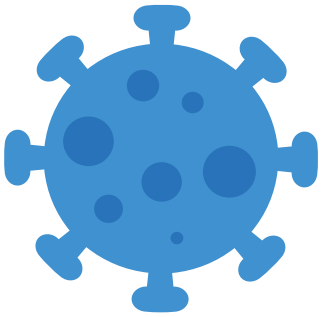


Phishing: Emails are sent to a wide audience in hopes someone will fall for the scam.



Spear Phishing: Emails are personalized and designed to trick a particular target. They are harder to recognize as fraudulent.

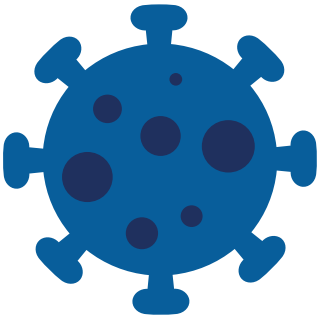
Phishing with COVID-19



New Ways to Lure You In

While the world is focused on the novel coronavirus, COVID-19, cyber criminals have adjusted their phishing lures to take advantage of the constant attention.

Bad actors mimic legitimate news and health organizations, such as the CDC and WHO, and provide links or attachments that claim to contain vital information about the COVID-19 pandemic. With so much information being spread about the pandemic, even those who wouldn't fall for a normal phishing attack may mistake these new lures for the real deal.



Always Be Skeptical!

Don't let curiosity or panic override your better judgement. Question any link or attachment about COVID-19, no matter who sent it.

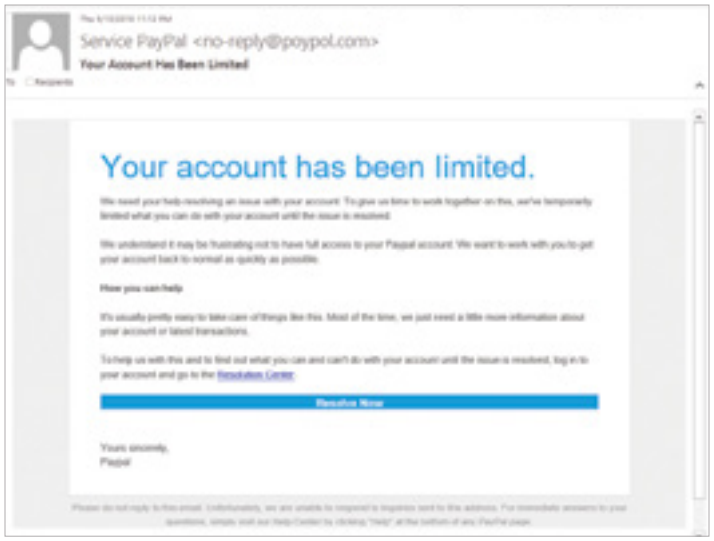
What to Do When You Recieve COVID-19 Emails

- ☒ Never open attachments about COVID-19. Legitimate agencies will include information in the body of an email, not attach it in a document.
- ☒ Do not click any links. If you feel the information could be legitimate, go to the organization's website manually, not by the link.
- ☒ If the email is from a known contact asking you to perform any type of financial transaction because they are home due to the lockdown or a positive COVID status, always call to confirm. DO NOT get confirmation by email.
- ☒ Never trust an email just because you know who sent it. Confirm with them verbally or though a messaging application if you think it might be real.

Your Email Best Practice Checklist ☒

The screenshots below show actual examples of spear phishing emails. As you can see, they look quite convincing. Fortunately, the act of opening an email doesn't usually do any harm. Clicking a subsequent link or downloading an attachment is what allows the criminal to infiltrate your system.
Click here to test your ability to tell the real from the fake.

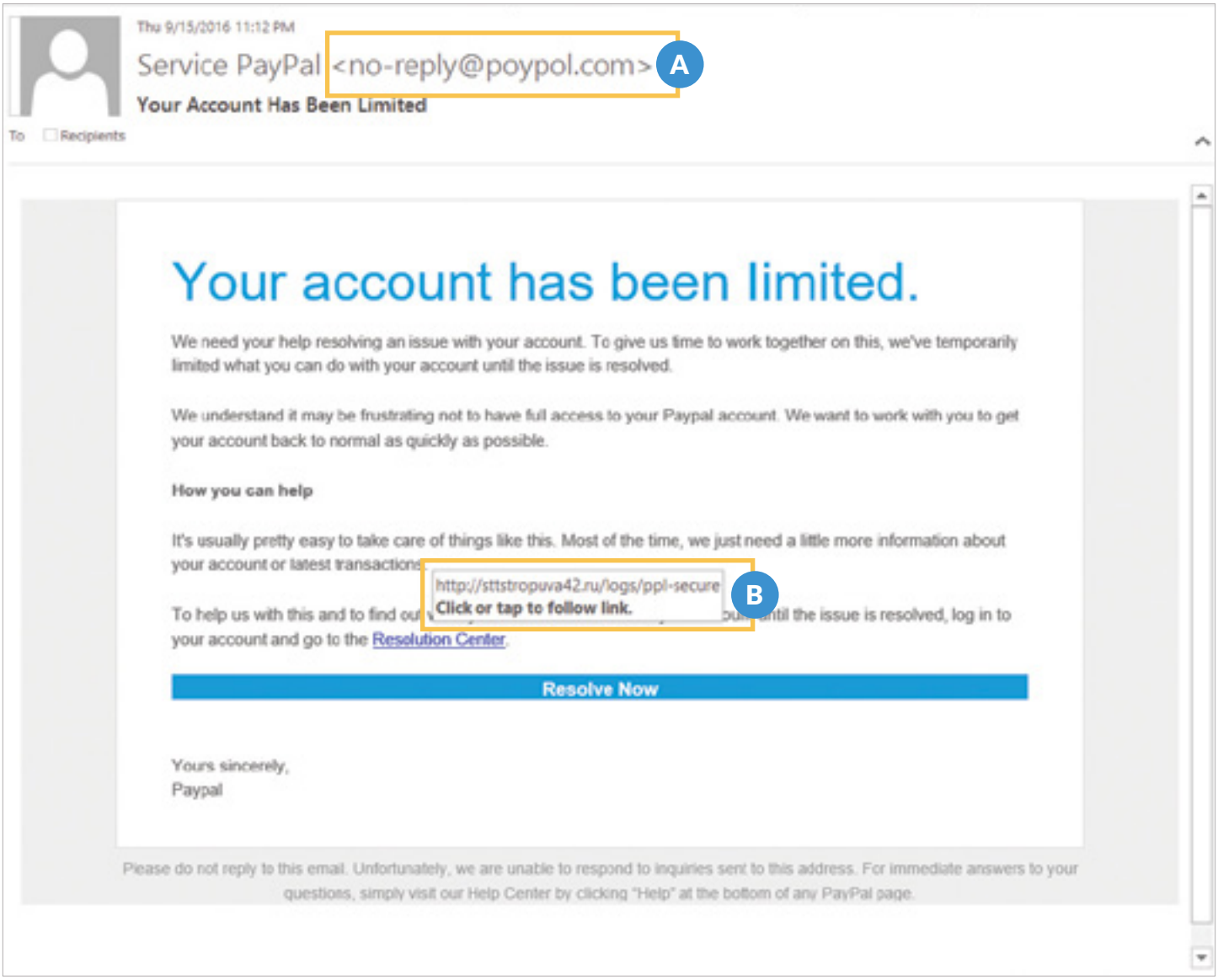
Actual Examples of Spear Phishing Emails



Your Email Best Practice Checklist ☒

Although spear phishing emails can be convincing, there are ways to identify them as fraudulent before you click a dangerous link.

Example A



A Incorrect Email Address

Examine the email address. Notice in this example, the email address uses "poypol.com" instead of "paypal.com."

B Suspicious URL

Hover your mouse over a link before clicking. Notice that although this URL includes the word "secure," it is actually leading to a website in Russia, as indicated by the .ru extension.

Your Email Best Practice Checklist ☒

Here's what you need to think about every time a new email hits your inbox.

1. Are they asking me for private or personal information?

Consider the nature of what the sender is asking for. Financial organizations will NEVER ask you to provide personal information like account numbers or passwords via email. Email is not secure. A legitimate bank will only ask for private information via a secure site after you have already proven your identity, ideally by a two-factor identification process (in which you take two steps to prove you are who you say you are, such as entering a password and answering a security question). Be alert if a sender is asking directly for personal information.

2. Does it seem too good to be true?

Phishing emails are sometimes recognizable because they promise something that seems too good to be true. Spear phishing emails are more subtle and realistic than phishing emails, so always be on high alert, remain skeptical, and remember, if something seems too good to be true, it probably is.

3. Where does this link lead?

Before clicking a link, hover over it with your mouse to see the URL. This can be a tip-off. If the URL does not match the sender's supposed company, be wary. Also be wary of URLs that end in domain names from foreign countries, like on the previous page in which the URL posing as a PayPal site actually directs to a website in Russia.

4. What is the email address of the sender?

Check the actual email address of the sender, not just the name that shows up during your inbox preview. Does the sender have a Yahoo address even though it claims to be with a business? Are there spelling errors, like the one in the "no-reply@poypol" example?

5. Are there attachments?

Attachments are a huge red flag! By downloading an attachment, you could infect your computer or even your entire business network with malware or viruses. Do not download an attachment unless you are certain of the sender's identity, and the content seems legitimate. If you weren't expecting to receive an attachment from the sender, even if you recognize the person, reach out by phone or other non-email channel to confirm it isn't malicious. If you do download an attachment, save and scan it with anti-virus software before opening it.

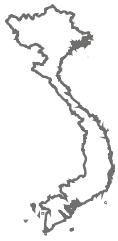
Country Domain Extensions Known to Be Cybercrime Hotspots

Russia - .ru

China - .cn

Brazil - .br

Vietnam - .vn



Nigeria - .ng

The Rules for Safe Surfing

Everyone needs to be mindful of web-browsing best practices. With one wrong click, you could infect your computer with dangerous malware that allows a criminal to affect your computer's performance or obtain personal information about you, your business, or customers. You cannot passively surf the web. Be alert, think before you click, and try not to visit sites you've never heard of. Here's what you need to know.

1. Seedy content breeds seedy behavior

Cybercrime is rampant on sites where people are doing something they probably shouldn't be. Pornography and anything illegal are prime targets for cybercriminals, in part because the sites' administrators probably aren't taking the steps necessary to protect their visitors. Stay off these types of sites—especially at work or when you are remotely connected to your work network.

2. Dangerous sites can show up in searches

Even innocuous behavior can land you in dangerous territory. Criminals create sites cleverly designed to trick users into believing they are legitimate. Plus, real sites can get hacked. Let's say you are searching for a gift on your lunch break and end up on a small e-retailer you've never heard of, a site that happens to have been hacked. A criminal could access your password and credit card information when you enter it on the affected site!

3. Use the "safe search" feature

Anti-virus and anti-malware programs often offer a "safe search" feature in which they'll run search results through their own database to rate the safety of sites and flag any URL they know to be compromised. If your business takes this security precaution, do not visit sites deemed unsafe by your anti-virus provider.

4. Install a firewall for enhanced protection

A firewall is a virtual fence between your network and the outside world and is designed to keep an attacker from accessing your network from an open port or protocol. An enterprise-grade firewall includes additional features that enable businesses to filter out certain types of content and add additional layers of malware protection. If you don't have a firewall, a managed services provider can help you set one up and provide the necessary ongoing maintenance of firewall settings. But remember, firewalls can't block everything, especially not zero-day threats, new attack vectors written to take advantage of previously undocumented flaws in a piece of software. Always stay alert and follow cybersecurity best practices.

(Continued on Next Page)

The Rules for Safe Surfing

(Continued from Previous Page)

5. Be careful about downloading things from the web

Cybercriminals do their damage by getting you to click a web link or download a nefarious attachment. The absolute safest approach would be to never download anything from the web, but we know in today's business environment that is not realistic. Proceed with caution, always scan files before downloading them, and if you are unsure if something is safe, run it by your IT partner or your manager first.

6. Exercise caution when working remotely

It's increasingly common for employees to work remotely, whether from home, a public place, or on the road as part of business travel. While this is certainly convenient, it poses major cybersecurity risks. Whenever you are using a company asset (such as a laptop, tablet, or smartphone), think before you connect to any Wi-Fi network. Even your at-home connection could be dangerous! If your home environment is not fully protected with up-to-date operating system patches, anti-virus definitions, firewall firmware, etc., it could be laced with problems. If you connect your company laptop, you could infect it and bring the malware back to your workplace.

7. Limit or eliminate browser extensions

Data leakage is a serious problem, especially when workers use their personal computers to access company data remotely. Browser extensions, even legitimate ones, can syphon data without the user realizing it. Avoid all unnecessary browser extensions to limit the risk to company or client data.

How to Tell If an Online Retailer Is Legitimate

1. Check for SSL Certification by seeing if the URL starts with HTTPS instead of HTTP. "S" stands for "secure" and means the site encrypts the traffic passing between it and your browser.

2. Make sure the site name looks legitimate, doesn't have strange spelling errors, and isn't trying to imitate a well-known site.

3. Confirm that the business the site represents has a physical address and phone number.

4. Check for a privacy policy, return policy, and other signs that the site is legitimate, such as a social media presence and user reviews.

5. Use common sense! If something seems too good to be true (i.e. the prices are incredibly low), be skeptical and leave the site.

So What Can the Bad Guys Really Do to Me Anyway?

There are a host of ways criminals threaten your personal security and your business. They steal personal information, steal business data, infiltrate your network so they can access other people's data, and even render your entire computer or network unusable. In ransomware attacks, perpetrators freeze users' computers or encrypt the data until they agree to pay a monetary sum. Ransomware attacks against small businesses are on the rise, so it is important your business takes precautions.

The Art of Password Management

In 2019, the most common computer password was "12345," followed by "123456," "123456789," "test1," and "password."[5] This is unacceptable! Cybercriminals use free software that can crack all standard passwords in just a few hours, and these obvious passwords are the first ones that the software tests.[6] Take the following steps to improve password security.

1.
Do not use the same password for everything.

2.
Create passwords with random words you can easily remember. Avoid obvious things like names of loved ones or birthdates.

3.
Revised guidelines recommend combining 4-5 words to create a long, strong password.

4.
Use a minimum of twelve characters. The longer the password, the stronger it is.

5.
Change your passwords periodically to stay a step ahead of unknown security breaches.

6.
Consider a password management tool to help you keep track of passwords.

7.
If you ever fear your cybersecurity has been compromised, change your passwords immediately.

Cryptojacking

Cryptojacking is a form of cybercrime that rose to prominence during the bitcoin explosion in 2018. While not as promenent now, it is still a threat to watch out for. Instead of attacking you directly, cybercriminals add code to a legitimate website. The moment you visit a webpage, your computer starts working for them.

What is Cryptojacking?

Cryptojacking is the method of using a victim's CPU processing power to mine for digital currency, such as Bitcoin or Monero. As the value of these currencies increase, so does the demand for more power to electronically mine for them, and this can have real-world consequences for you. Over-taxed computers and overheating phones can impact how well your business performs.

What to Watch Out For

While it's not always apparent you've been cryptojacked, there are warning signs and steps you can take to keep your computer safe.

- Know how to check your CPU usage. A sluggish computer is the first sign. If your browser is using nearly all your CPU power, that's not normal. Close your browser and see if your usage returns to normal.
- Don't ignore a hot phone. An overheated phone battery is a sign of high power usage and can even result in explosions. If there's no reason for the sudden increase in power consumption, contact your IT provider.
- Listen to your computer's fan. Just like a phone, your computer runs hot when it's using power and will try to cool off. If your computer's fan is running loudly all the time, you should investigate the root cause.
- Maintain updated anti-virus, anti-malware, and ad-blockers. Most scripts used in cryptojacking are recognized by the security plugins and ad-blockers you can install in your browser. Keeping these updated and active is the best way to avoid cryptojacking altogether.

“Uh-oh!”

What to Do When You Think Your Cybersecurity Has Been Compromised

Following digital best practices will help you avoid cyber threats, but the bad guys are so sneaky that they can trip up even the most cautious among us. Mistakes happen.

Sometimes a virus will go completely unnoticed. Other times, it may affect computer performance, especially if you have an older machine.

If you click a link and don’t feel comfortable with where it leads or what pops up, download an attachment and are apprehensive about what happens next, or simply feel unsure for any reason, trust your instincts and take the following steps.

- Call your IT partner at any time if you need assistance.
- Don’t click anything, not even an “X” to close a pop-up box.
- Disconnect from the network by either physically removing the network cable if your machine is hardwired or by turning off your computer’s Wi-Fi connection.
- Reboot your computer in Safe Mode and run a full system scan with your anti-virus and anti-malware software.
- If an unresolved issue is identified, ensure you have an existing backup of your data, reformat your hard drive, reinstall the operating system, reinstall all third-party software, and restore your data from the known good backup.
- Perform a second system scan to ensure your machine is clean.
- Update all critical passwords. Monitor your sensitive data and financial accounts.

If you didn’t actually click the harmful link or download anything dangerous, a simple reboot may be all you need. If everything appears fine, ensure your anti-virus and anti-malware software is up-to-date and run a full system scan. Clear your browser cache (a good step to take routinely anyway) and change your passwords for extra security.

“X” Does Not Mark The Spot

If you are suspicious of a pop-up, don’t try to close the window by clicking the “X”! Even though you are trying to dismiss the threat, the simple act of clicking could be enough to infect your computer. Instead, disconnect from your business network and call an IT expert right away.

The Bottom Line? Be Skeptical.

Be skeptical about every email you receive and every website you visit.

Do not move passively through the digital realm. Liken it to a bustling foreign bazaar with a notoriously high rate of theft. You wouldn't go around giving personal information to every random person who asked.

Stay alert and think before you click.

Endnotes

[1] Help Net Security, "In 2019, a total of 7,098 reported breaches exposed 15.1 billion records," accessed May 5, 2020. https://www.helpnetsecurity.com/2020/02/11/2019-reported-breaches/

[2] Datto, "Datto's Global State of the Channel Ransomware Report," accessed May 6, 2020. https://www.datto.com/resources/dattos-global-state-of-the-channel-ransomware-report.

[3] C, Eric, SafetyDetectives, "Ransomware Facts, Trends & Statics for 2020," last modified April 22, 2020. https://www.safetydetectives.com/blog/ransomware-statistics/.

[4] SelfKey, "All Data Breaches in 2019 & 2020 - An Alarming Timeline," last modified April 7, 2020. https://selfkey.org/data-breaches-in-2019/.

[5] WeLiveSecurity, "The worst passwords of 2019: Did yours make the list?," last modified December 16, 2019. https://selfkey.org/data-breaches-in-2019/.

[6]Poston, Howard, Infosec, "10 Most Popular Password Cracking Tools [Updated 2020]," last modified September 25, 2020. https://resources.infosecinstitute.com/topic/10-popular-password-cracking-tools/

About Anderson Technologies

We hope you found this handbook useful. Educating yourself and your team is an integral and often overlooked component of cybersecurity.

If you are concerned about IT security and are looking for a trusted partner we can help. Anderson Technologies' team of experts specialize in defending and safeguarding small businesses. We'd love to learn about your IT challenges to determine if we are a good fit.

Click to Schedule a Free Consultation

Click to View All Our Free Resources

Have Any Questions?

The team at Anderson Technologies is happy to discuss any questions you have or schedule a time to help educate your employees about best practices. Give us a call today at 314.394.3001.

ANDERSON TECHNOLOGIES