

CYBERSECURING OUR FUTURE

QUARTERLY

ed. 2

BIZCOM GLOBAL

919-855-8399

[HTTPS://BIZCOM
GLOBAL.COM/](https://bizcomglobal.com/)



MANAGED CLOUD, IT & CYBERSECURITY



DISCOVER INSIDE...

06

*supply chain
threats grow
and zero-
trust solutions*

11

*is your favorite
social media
secure?*

14

*game or gamble?
the latest social
engineering
threat*

17

*unseen threats
and finding your
biggest
blindspots*

23

*threats
dominating
2023*

25

*deepfakes and
deep learning
AI*

26

*common
crypto scams
and threats to
your digital
wallets*

29

*most common
brands faked
by phishers*

32

*is phishing
really that
dangerous?*

INTRODUCTION

Hi!

By picking up this magazine, you've already taken the first step to becoming more cyber-secure in your everyday life! BizCom Global is happy to bring you the latest updates in the cybersecurity industry EVERY QUARTER because the more you know, the better protected you'll be - in your personal and professional life!

Think about the state of the internet when you were born versus where it's at today. Pre-internet and old dial-up computer users remember how it was before smartphones were in every pocket, tracking your every move and helping people navigate every aspect of their busy, modern lives.

Technology is not just here to stay. It is constantly advancing and evolving. How is that changing our approaches to cybersecurity?

That's what we're here to investigate for you.

LET'S GET STARTED



ABOUT US

First, we want to thank you for picking up this magazine and joining the fight against cyber-threats to you and your business! Education is the first (and most important) step toward preventing insider and outsider threats from attacking your personal data.

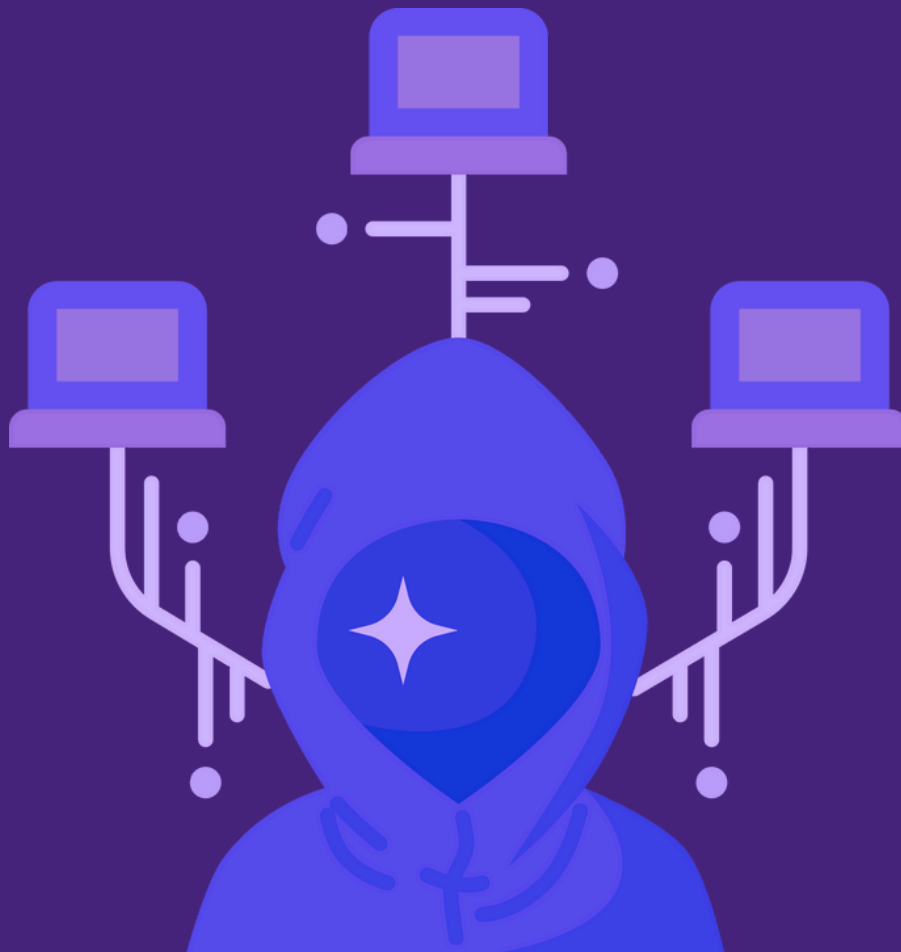
That's what we do here at BizCom Global.

Since 2003 we have successfully worked with numerous small and mid-sized businesses. Our mission is to provide our customers with constructive technology tools and strategies in order to facilitate improved employee productivity and company growth, while fiercely protecting the underlying organization, its systems, and data, and helping to ensure compliance with the growing number of regulations nationally and internationally.

Bringing you this magazine every quarter is our way of bringing accessible cybersecurity tips and industry knowledge right to your inbox!

"Time is what determines security. With enough time nothing is unhackable."

- Aniekee Tochukwu Ezekiel



SUPPLY CHAIN THREATS GROW

what they are & how to avoid them

As the world has gone digital, the supply chain risks have only increased. The digital super-highway provides extensive information availability, and enables communication and collaboration because of the technological integration of systems and processes, **thereby interconnecting every integral part of a supply chain.**



The more complex a supply is, the less predictable the likelihood and the impact of disruption are. In simple words, the probability (likelihood of risk occurrence) of risks is very high given how advanced international and global supply chains are now.

Unfortunately, **we are all susceptible to supply chain attacks because we tend to trust the services that we know and have used for years.** It's a perfect way to sneak onto important databases and exploit systems that would otherwise be tough to brute-force into!



MORE TELECOM BREACHES EXPOSED

Recently, AT&T has been in the news due to a data breach that exposed sensitive customer information and caused potential financial losses.

Currently, AT&T provide services to over 100M customers, and have been in operation for more than a century. They have a lot of resources to develop cyber-defenses, but **none of that matters if their suppliers are compromised.**

Meanwhile, their internal databases do not appear to have been affected. The threat actors did, however, manage to steal information on 9M users — that's **nearly one out of every ten customers.** Exposed information includes names, account information, phone numbers and emails.

The company has taken steps to mitigate the damage and protect its customers' data by implementing new security measures and increasing its focus on cyber safety. In the past, they've also provided customers who were potentially affected by data leaks with free credit monitoring services.

Unfortunately, breaches on third-party suppliers and on telecommunication companies are both on the rise. ***Supply chains and the telecom industry seem to be staring down a cybercrime epidemic.***

What can you do? ***Keep your security awareness strong. Report suspicious behavior when you see it, either online or in the office itself.*** Monitor your accounts, bank statements and credit if you may have been affected.

Talk to your IT provider about best practices and what to do before you act. When in doubt, err on the side of caution.



Similar attacks have been happening all over the world, from the Telus breach in Canada to the Australian breach against Optus to the homefront attacks on Google Fi and T-Mobile.

These have all occurred within the past six months.

”

WHEN IN
DOUBT, ERR
ON THE SIDE
OF CAUTION.

IF YOUR DATA IS EXPOSED

If you receive a notice that your data has potentially been exposed in a breach, take action immediately. This includes making sure that you change any passwords associated with the breach, monitoring your bank accounts for any suspicious activity, and most importantly, NOTIFY YOUR I.T. PROVIDER so they can give you expert recommendations on what to do next.

QUICK REMINDER

Passwords should be changed *at least every 2 months* regardless. Use *at least 12 characters* of letters, numbers and symbols!



THE SOLUTION? ZERO TRUST.



Consider a **Zero-Trust framework**, which is an approach to IT security that assumes no user, device or service is trustworthy. It focuses on *verifying the identity of users and devices before granting access to a network or system*. With the Zero-Trust framework, organizations can protect their data by using multiple layers of security controls and continuous monitoring services on their networks.

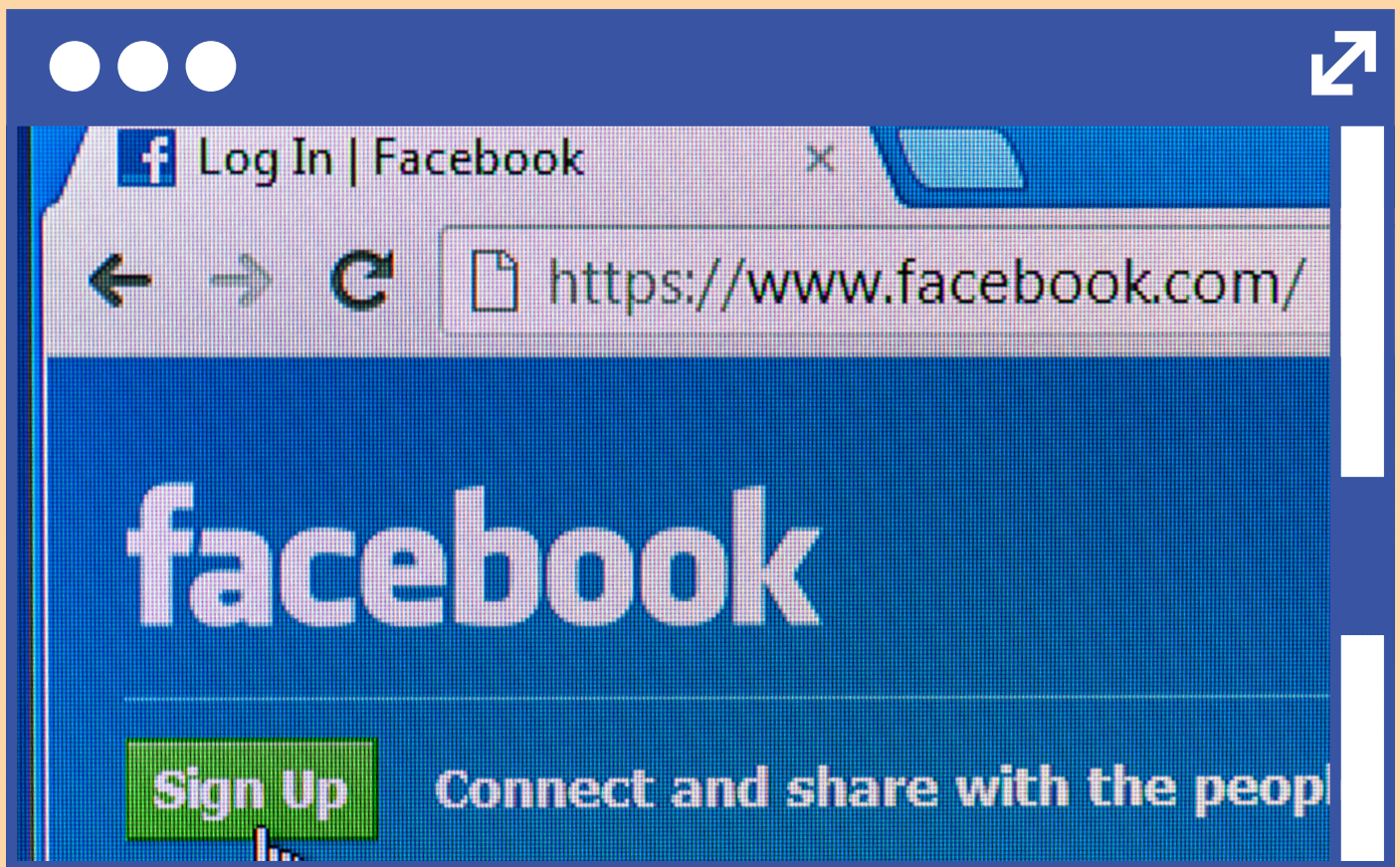
This approach helps them reduce the risk of unauthorized access and data breaches. The Zero-Trust framework also provides organizations with **more granular control over user access**, allowing them to limit access based on user roles and permissions.

By implementing Zero-Trust, organizations can ensure that only authorized users have access to sensitive data while protecting against malicious actors who may try to gain unauthorized entry.

Zero-trust accounts for devices which may be better security risks, and protects the bulk of data if some is exposed.

"Social engineering bypasses all technologies, including firewalls."

- Kevin Mitnick



IS YOUR FAVORITE SOCIAL MEDIA SECURE?

Do you know the top five most popular social media platforms in the world?

1. Facebook
2. YouTube
3. WhatsApp
4. Instagram
5. TikTok

We all use social media. The platform we prefer might differ, but **59% of the people around the globe have some form** of it. Chances are, you do use an app to connect with friends online, too.

Facebook

Facebook has a lot of settings that can be toggled on and off, depending on how much data you want to give it. From geo-location services that help you check into different places, to facial recognition for easy tagging in photos, to the cookies it collects to run sidebar ads relevant to your interests, the platform can keep a lot of data on you if you let it.

YouTube

It may not surprise you that YouTube can see everything you search on the website, from the videos you watch to the playlists that you like. Tracking what you enjoy watching and how long you sit through videos helps the site make better recommendations on what you should watch next, with the goal of keeping you browsing and engaged. That's also why they ask your opinions on ads that pop up before some videos; it's all to personalize the experience.

Remember, though, YouTube is owned by Google. All of that data goes back to the mega-corporation, adding to their big picture of who you are (and all that backstory informs their video recommendations in return).

WhatsApp

On the plus side, WhatsApp is end-to-end encrypted. That basically means that the messages are secured from your device to the recipient's; they're also scrambled as "tokens" that can't be read unless decrypted, so the communication is protected even in transit.

That doesn't mean that the platform isn't collecting data on you, however. The database saves your messages, the timestamp, and who was in the message thread. That can all be accessed later.

Did you know? The app can also access location services, your contact list, and all of your media too! Be careful what permissions you toggle on whenever you download a new app.

Instagram

A few years ago, Facebook actually bought Instagram, so a lot of their data collection methods are similar. Meanwhile, this collaboration also means that Facebook can access your Instagram data and vice versa — which doubles the amount of information that you could be inputting into the same database, without realizing it's all going to the same place.

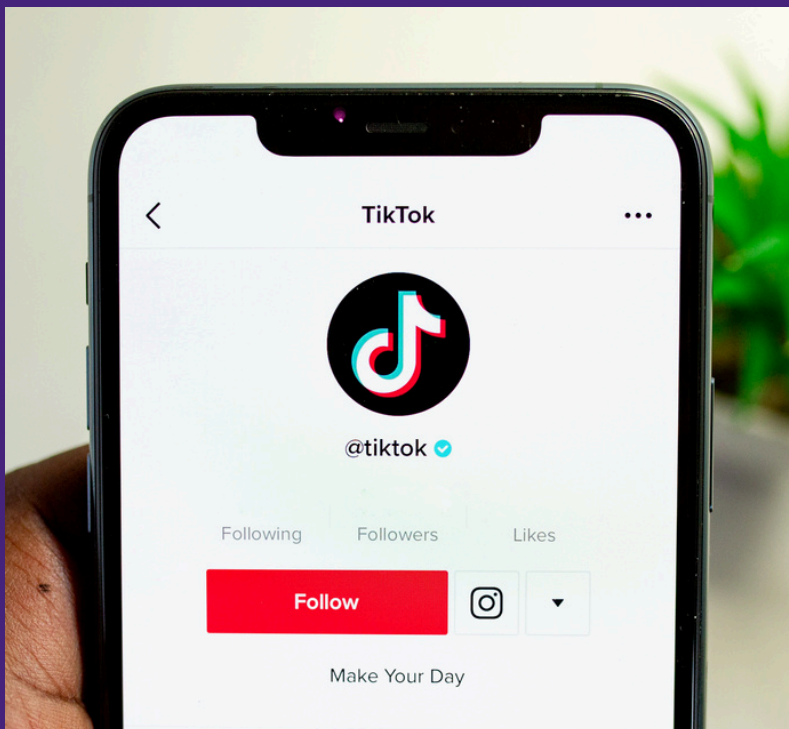
Plenty of people also use Instagram to shop online or learn about worldwide news. Instagram also takes into account what you look at and how long so as to send more personalized ads to your feed.



TikTok

A string of controversies concerning data mining and privacy leaks on TikTok have made headlines in the last few years, but that doesn't seem to be slowing the app down much: It currently boasts over 1B users worldwide, compared to 655.9M just two years ago.

Despite the wide audience, tech researchers have found that TikTok can do all sorts of covert tracking across all your apps and networks, although the social media app refutes these data collection claims. It has also been criticized for its lack of safety measures and unwillingness to suspend user accounts deemed to be engaging in predatory behavior, which is particularly concerning given the apps' appeal to a mostly younger demographic. Although children under 13 have additional privacy settings on their profiles, there are still safety concerns; and anyway, we all know how easy it is to fake our ages online.



CONVENIENT
OR CREEPY?

THAT'S UP
TO YOU TO
DECIDE.



GAME OR GAMBLE?

*beware this new social
engineering threat*

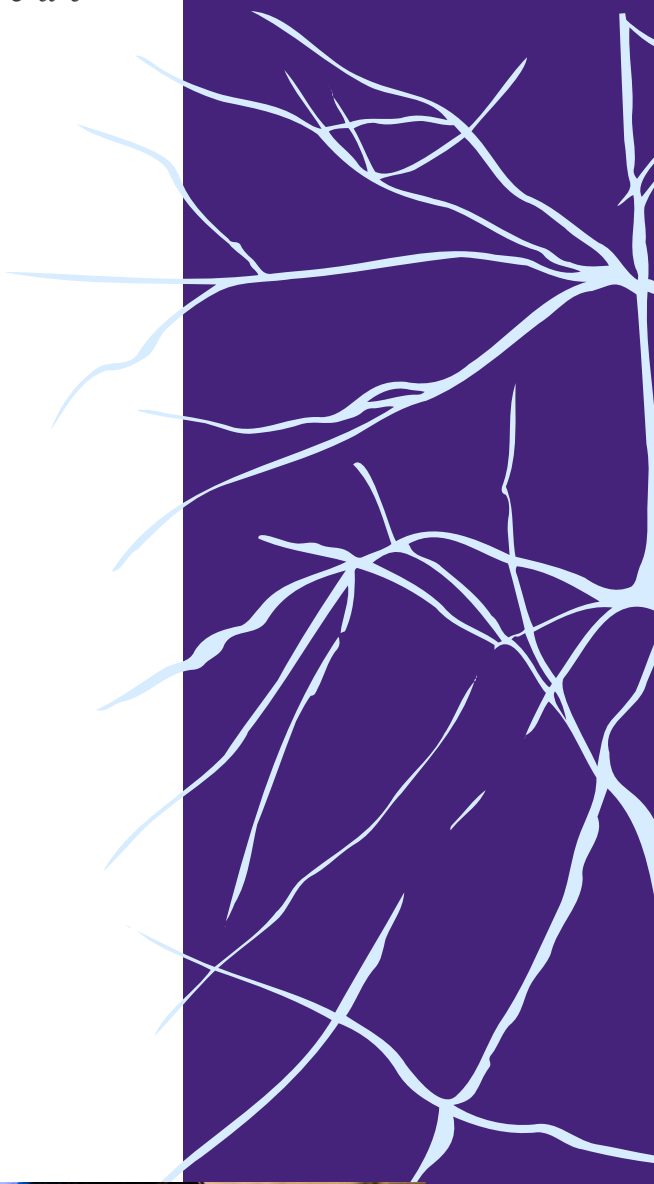
Ice Breaker.

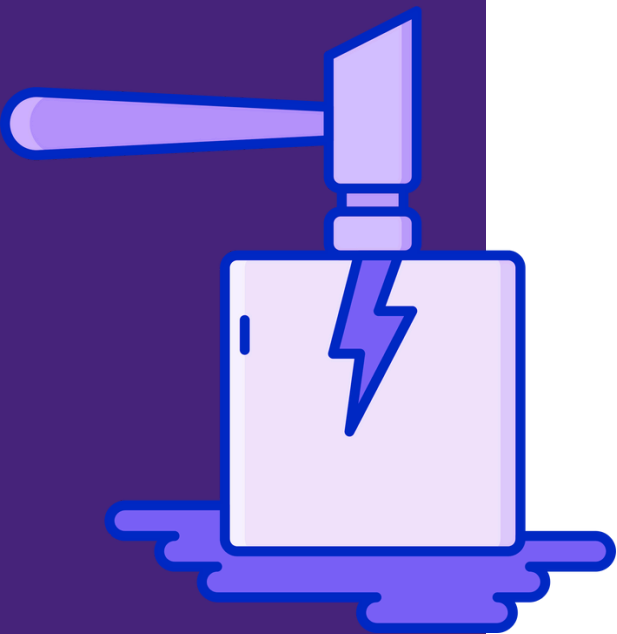
No, not the kind that you play during team building exercises. This is the name of a recent social engineering threat that has emerged in the past few months. They play on emotions to get their target to react without thinking, in a way that allows the threat actor to gain access to your accounts or systems.

The problem is, it's not you that they're targeting this time.

Security experts in Israel first noticed the multi-step threat in September 2022, and the attacks have only grown more prevalent since. Gaming and gambling events are beginning soon, such as the ICE London 2023 game convention in February (which is actually where the threat got its name) or any given night in Las Vegas.

Whichever one is your hobby, watch out for any suspicious activity on your accounts while we're still learning more about how this threat works!





The cybercriminal starts by pretending to be a customer with an online platform of some kind, like a digital casino or tournament site. They contact the support team there, sounding like a non-native English speaker and requesting to talk to someone else who is too. This is to decrease the chances of getting flagged as a scam. To worsen the odds further, many online platforms in the gaming and gambling industries tend to outsource their customer support, so they can't necessarily impose their own security awareness training and warn about these kinds of tricks.

Once the threat actor is on with support, they'll send a screenshot of a supposed problem that they're having and ask for help resolving it. The "picture" is often sent through external platforms like Dropbox, or a fake screenshot hosting website.

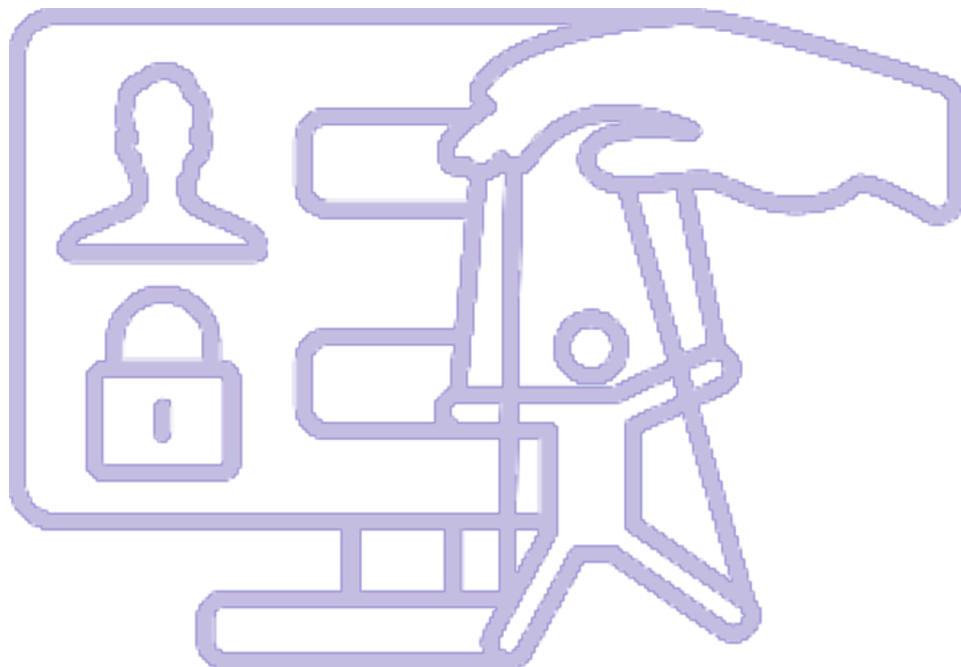
Only when the team member clicks on the link, it doesn't open a JPG — instead malware instantly begins to download and start running.

After the malware has been downloaded onto the customer support agent's system, it creates a backdoor through JavaScript. This allows the hacker to run processes, steal data, move or take files, and really wreak whatever havoc they like.

Gaming and gambling are common targets for cybercriminals, since there's always money in a tournament or casino. You should always be careful when entering payment info online, but especially if the purpose of the platform is to hold large amounts of money. It's a natural target for thieves, that puts your accounts, funds and privacy at risk!

"It is far easier to concentrate power than to concentrate knowledge. That is why so much social engineering backfires and why so many despots have led their countries into disasters."

- Thomas Sowell, *"Intellectuals and Society"*



UNSEEN THREATS CAN MAKE THE BIGGEST SPLASH



SPYWARE

the three types of spyware



AD-WARE

If you've been getting incessant advertisements popping up on your computer screen no matter what websites you visit, or your usual web browser is acting suspicious some other way, then you might be infected with adware.

It's a form of malware that tries to get money by offering bogus scams that appear to come from legitimate products, but actually come from an infected software that's been secretly downloaded to your device.

INFO-STEALERS

After surreptitiously downloading onto your system, the infostealer begins to funnel precious information back to whomever launched the attack.

They can take data like your login usernames, passwords, and even cookies that tracked your browser history!

KEYLOGGERS

Much like infostealers, keyloggers are secretly downloaded onto your device and deliver all their discoveries back to the hacker.

They can read every keystroke that you make. If you type in your bank routing number, it can see that. If you enter your SSN, they can see that too. You quickly see the dangers inherent in keyloggers that you don't know are there!

KEYLOGGER 101

Keylogging technology records and stores the keystrokes entered on a computer. It's not all malicious: It's used for some content filtering purposes, such as monitoring employee activity, tracking user behavior and collecting data for research. However, these trackers can also get onto your systems if they come in packaged with malware, or a cyber-criminal manually installs the program once they've somehow gained physical access to the machine.

What if threat actors could see everything that you did online? Everything you searched, every message you sent, every password you entered?

If your device is infected with the right software, then this nightmare can become all too real!

It's not just your search history at risk if this information falls into the wrong hands.

The collected data can be used to gain access to passwords and other sensitive information stored on the computer.

The good news is, we are not defenseless against malicious keylogging! Antivirus software and continuous monitoring services can help weed out intruders on your network and purge malware from the system.

What if the tracking software compromises your accounts before you notice and purge it from the system? Multi-factor authentication can help here. Even if a threat actor were to steal your log-in and password, they wouldn't be able to access your one-time code, fingerprint or whatever other form of secondary identification you use to log in.

As scary as this sounds, ***you are not defenseless! We are equipped to protect*** your network and all the systems on it.

THE MORE YOU KNOW:

80% of keyloggers can't be spotted by antivirus software and firewalls

300+ kinds of keyloggers can be leveraged against you

10M U.S. computers are infected with keyloggers right now

67% of employers use keyloggers or other monitoring software on their employees


FINDING YOUR BIGGEST BLINDSPOTS

When dealing with threats that might be harder to spot, like keyloggers and info-stealers which can go undetected until your continuous monitoring services find your PII already on the Dark Web, it's important to know where your biggest network vulnerabilities lie.

Risk assessments use detailed, administrative questions to determine someone's risk of imminent breach given the current threat landscape. Usually, these pull from global, real-time databases to provide the most effective recommendations for patching these vulnerabilities before they can be exploited.

Vulnerability assessments similarly pull from global databases. Then a scanner interrogates all devices attached to the network, seeking out and testing them for all vulnerabilities. Basically, everything is assumed exploitable until proven secure.

Penetration tests find out how deep a hacker could dive into your network, depending on the most common threats to your industry, existing holes in your attack surface and the effectiveness of your incident response plan.



If you don't invest in risk management, it doesn't matter what business you're in, it's a risky business.

—Gary Cohn



THE MORE YOU KNOW...

| 1.9K

*CVEs are found
on average
each month*

| 33%

*of vulnerabilities
are highly to
critically severe*

| 65K

*vulnerabilities
were found in
2022*

ETHICAL HACKING

Why wait until someone actually does your business harm? Ethical hacking is a chance to catch vulnerabilities before they're exploited in earnest.

These "white hat hackers" go through the system just like if they were a bad actor: They find vulnerabilities, exploit backdoors, and pretend to perform malicious activities. They might send test phishing emails, try to access privileged folders, and even set up denial-of-service attacks. This also tests how well employees follow their incident response plan!

Forms of ethical hacking stretch back decades, though its eruption into the private sector has made it much more commonplace as well as more widely-known as an available option.



"We shouldn't worry about getting hacked; that's illegal."

- Unknown



THESE THREATS ARE DOMINATING 2023:

✓ *Ransomware* tops the chart again this year as one of the most expensive threats and damaging you can encounter

✓ *Supply chain attacks* have become one of the most serious threats to individuals and businesses alike

✓ *Deepfakes* and other cutting-edge AI technology that can imitate real people and be alarmingly convincing

✓ *Crypto-related scams* like cryptomining, -jacking and ATM hacking

THE
YEAR
SO
FAR...



Deepfaking is a malicious practice that presents one of the biggest concerns about AI today.

The name comes from **deep learning AI**, which basically fills a database with information that the artificial intelligence can use to, well, get smarter!

Deepfake technology teaches their algorithms how to identify certain individuals and then replace their visage with someone else's, in both picture and video format. They can even source audio clips to make these likenesses "talk!"

This kind of AI becomes more accurate over time, as it learns to recognize mistakes and gets fed more reference images. That means deepfakes will only get more and more convincing with time!

Would you fall for a catfish this good?

2X

the amount of expert-level deepfakes doubles every six months

71%

of people around the world don't know what deepfaking is

82

applications exist to deepfake pictures and videos

DEEPPFAKES



COMMON CRYPTO SCAMS

protect your digital wallet

CRYPTO- JACKING

Cybercriminals can use someone else's computing power to mine for cryptocurrency. It uses up a ton of electricity on the victim's end, thereby slowing down your device and using up tons of power

CRYPTO EXCHANGE HACKS

Crypto exchanges allow you to buy and sell digital currency. When these exchange systems get hacked, it affects the platform, investors and everyone who uses the exchange. They don't often recover the stolen crypto, either.

DIGITAL WALLET COMPROMISE

ONLY access your funds from secure devices to reduce the risk of picking up malware that compromise credentials. Hackers could break directly into your digital wallet and transfer all your cryptocurrency to themselves!



DID YOU KNOW?

*cybercriminals can create
fake digital tokens!*

In a "rug pulling" scam, threat actors create fake digital tokens that mimic legitimate cryptocurrency, like Bitcoin, Ethereum, Tether, etc. Unlike real tokens, though, the tokens are completely defunct. In other words, they're worthless.

Here's how they do it. First, the cryptocurrency creator advertises heavily to get people to invest in their tokens. Once they've collected enough to satisfy the threat actor, they simply...disappear with all the funds that they've collected.

Not only does the creator of those fake tokens effectively make that digital money worthless, but they're often accompanied by specific code that prevents outsiders from selling the token to anyone else. No passing the buck!

"One of the main cyber-risks is to think they don't exist. "

- *Stéphane Nappo*



MOST COMMON BRANDS FAKED BY PHISHERS

when we get smarter, thieves get savvier

Cyber-thieves love to use the names of big corporations in their phishing campaigns. If they're spamming large swaths of people, then picking a disguise like Microsoft or LinkedIn increases the odds that more people will at least *use* these services.

Think about it: If you get an urgent message about your car insurance when you don't even own a vehicle, it's pretty obvious that's a scam. That's why cybercriminals will often choose to impersonate companies that have millions of users.

So...can you guess who's the #1 impersonated brand in 2023?

Walmart.



Does that surprise you? It might: At the tail end of 2022, Walmart only ranked #13 in a study by *Check Point Research*.

This traces back to a scam perpetuated by threat actors, "warning" Walmart customers of a potential disruption to their supply chain that may affect shopping and ordering. This false notification was followed by a survey link, which really downloaded infected software.

This is a prime example of why threat actors impersonate big corporations to trick more people at once - rather than **spear-phishing** attacks which are more specific but also more believable as a result.

By mimicking Walmart, the threat actors would have plenty of real customer service emails to comb through and use as a convincing template.

WHO ELSE MAKES THE LIST?

Following Walmart, the most common brands that phishers have been faking this year:

✦ *DHL* mail courier service

✦ *Microsoft*

✦ *LinkedIn*

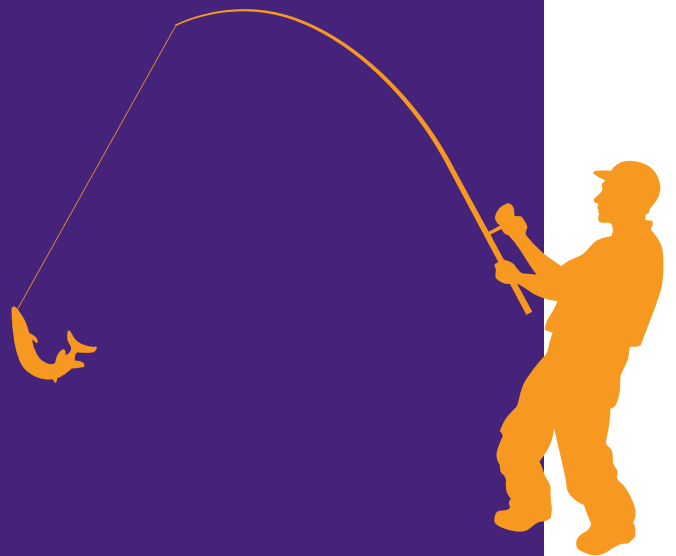
✦ *FedEx*

✦ *Google*

✦ *Netflix*

✦ *Raiffeisen*, a European universal bank

✦ *PayPal*



SPEAR-PHISHING

Security awareness training has fortunately taught employees across all kinds of industries how to recognize and avoid phishing attempts. You might have even gotten some training in avoiding them, yourself. How much, however, do you know about one of its sinister subsets: **Spear phishing?**

While some of the hallmarks of a phishing message includes not directly addressing you by name or making unspecified claims meant to scare you into action, but you won't find many of those mistakes in a spear phishing message. Instead, spear phishing is an email scam that is directly targeting you, your organization or job. It is designed to hack into your particular computer, so you can bet it's designed to play on your particular weaknesses.

76% of all phishing attacks carried out are now targeted, spear-phishing campaigns.

Source: Slashnext's 2022 State of Phishing Report

Spear phishing is a type of social engineering attack where the hacker has narrowed you down to the most approachable target, the one with the access to the files they want, and they craft a message specifically designed to ensnare YOU.

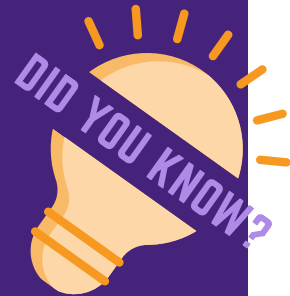
The best defensive move that you can make on a daily basis is to **stay vigilant** and learn how to recognize new threats and scare tactics as they crop up.



IS PHISHING REALLY THAT DANGEROUS?



*case study:
the attack
on Reddit*



Reddit has
330M
*active monthly
users*

Even if 99% of the organization flags and reports spam, that 1% can send the whole organization crumbling down. So when a determined cybercriminal had been inundating Reddit workers with messages leading to fake websites that they set up to look like the internal portal that Reddit employees usually use for work, the persistence and likeness fooled one employee.

When the victim logged in, they inadvertently handed over their login credentials and multi-factor authentication tokens. Due to just that one slip-up, that one time somebody didn't recognize a phishing scam for what it was, the attacker was able to swipe confidential files, bits of code, and some internal business systems too!

This is a prime example of why security awareness is a 24/7/365 responsibility!

This is not the first major breach to affect a big website in 2023. The cyber-threat landscape is becoming increasingly treacherous, and companies of all sizes will be targets.

If you are notified that your data has been compromised, or may have been exposed in a breach, take immediate action to re-secure your accounts and monitor your credit, systems and profiles for suspicious activity!



"There are only two types of companies: Those that have been hacked, and those that will be."

- Robert Mueller

CYBERSECURITY YOU CAN TRUST!



We believe in providing YOU the best-in-class security suite to keep you cyber-secure in the face of an ever-changing threat landscape.

Call us today at **919-855-8399** and let us help you wrap a security blanket around your business.



MANAGED CLOUD, IT & CYBERSECURITY