RAZZ
PROFESSIONAL SERVICES

Cybersecuring OUR FUTURE

Vol.2

What it takes to be **cyber-secure**

Cybersecurity in the news: ChatGPT leaked

Gen Z vs Cyber-safety

Unraveling threads

SECURITY EVERYWHERE YOU GO:

How to make your **mobile devices** more secure

info@razzpro.com | (310) 695-2199 | razzpro.com

CONTENTS

INTRO DUCTION

The digital world is everywhere, and hard to understand! Don't you sometimes wish that you had a handy guide for what was going on in the world of new technologies?

Online technology has the unique privilege of making extremely big strides in a short period of time. Think about the state of the internet when you were born versus where it's at today. Pre-internet days 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.

It's a phone, camera, calendar, email, game and browser all rolled into one. You can literally access any information you want at any given time. How many times have you touched your phone in the past hour?

For better or worse, technology is here to stay. That's why this magazine is launching, to bring you the **latest news about cyber-threats**, and the legislation and security features that are coming out to combat these dangers.

How is the landscape of cybersecurity changing? That's what we're here to investigate for you.

LET'S GET STARTED

ABOUT

WHO IS RAZZ PRO?

Meet technology expert and CEO, Ty Romstadt! He is on a mission to bring you the latest in cybersecurity news and events! Here's a personal message from him:

First, I 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.

Our mission at Razz Pro is to encourage and educate as many businesses as possible on current and best practices when it comes to cybersecurity.

For a sense of cybersecurity now and going forward, here is: *Cybersecuring Our Future.*

"Good help is hard to come by, especially when it comes to technology and IT security. Razz Pro breaks it down and makes it easy and stress free through their expertise and dedication to customer service. No matter what level of assistance you are looking for, Ty will help develop a plan and approach that is tailored just for you."

Troy Ritter Vice President of Chartered Development Corporation

"THE FRAUDSTER'S greatest liability is the certainty the fraud is too clever to be detected."

-Louis J. Freeh, Former Director of the FBI

CHATGPT LEAKED

More than 100K user accounts had their data leaked in a massive exposure that had been ongoing for over a year.

The well-known spyware, Raccoon Stealer, claimed to have disbanded in 2022 but it appears that their malware is still alive and well.

From June 2022 to May 2023, 101,134 ChatGPT user accounts were EXPOSED!

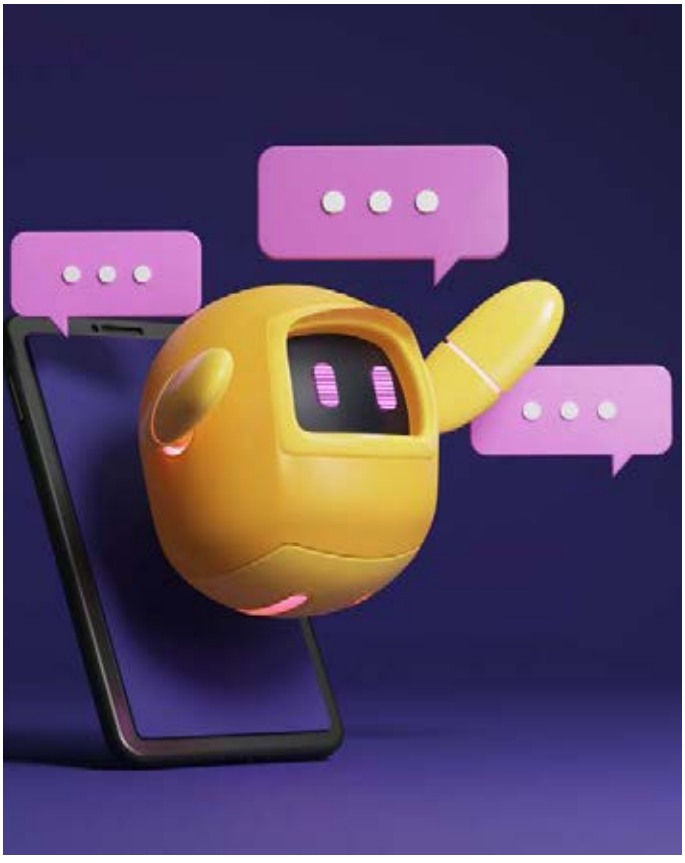
> "101,134 CHATGPT USER ACCOUNTS WERE EXPOSED!"

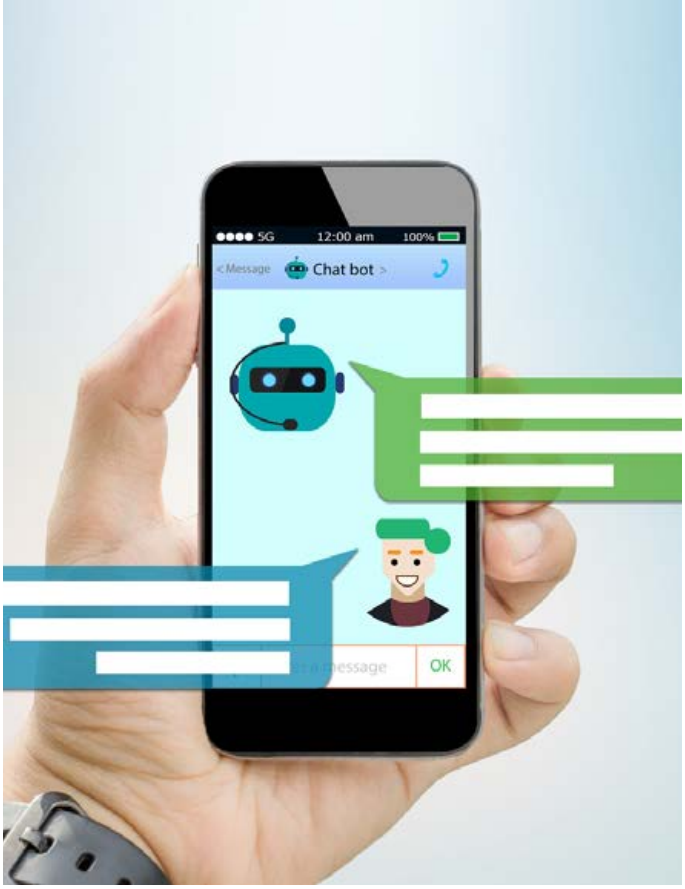
Whenever new software is adopted as swiftly and widely as ChatGPT artificial intelligence has been, there are guaranteed to be threat actors looking for exploitable vulnerabilities.

Now we are seeing the results of this. Impacted countries include the United States, Pakistan, France, Brazil, Vietnam, Morocco, Egypt and Indonesia.

Data stolen from users included emails, credit card information, cryptocurrency wallet logins and logged archives.

By prioritizing security and taking proactive steps during the rapid adoption of new software, you can better protect your systems and data from potential cyber threats—while still enjoying everything new technology has to offer.





If you're one of the many people around the world eager to adopt new software, take proactive steps to protect your systems:

- Conduct security assessments and evaluations before deployment
- Regularly apply security updates and patches as they become available
- Configure security settings to align with best practices
- Refresh your training to promote awareness and secure usage
- Monitor and promptly address any compatibility issues
- Engage with vendors and developers to ensure ongoing support and prompt response to security concerns
- Implement robust security measures such as firewalls, intrusion detection systems and secure network architectures

GEN Z VS CYBER-SAFETY

Who would win?

They'll make up nearly a third of the workforce by 2030.

Most of them have had access to the internet since before they could talk.

We're talking about Generation Z — in other words, everyone who was born between 1997 and 2012.

Because they were born smack in the middle of the digital boon, Gen Z has grown up alongside advancing technology. As a result, they tend to have a heightened awareness of privacy and data security issues. They are often more cautious about sharing personal information online and are concerned about the potential misuse of their data. These are concerns they've been dealing with their whole lives!

On the other hand, their submersion in technology since birth also creates some apathy and jadedness about how much of their data is really "private."

Consider the early-2000s advice: "Don't post any real information online!" Now, family vlogs capitalize on every new life stage their children reach, and TikTok is awash with strangers giving out their full name and showing their daily walk around their neighborhood.

A 2020 study by the National Cyber Security Alliance found that 74% of Gen Z actively manages their social media privacy settings.

61% of Gen Z respondents regularly use security tools like two-factor authentication (2FA) to protect their online accounts. This was higher than any other age group surveyed!

It's possible to utilize the many great qualities of the internet without risking our digital and physical safety.

EVERYONE can all use the security awareness knowledge and reminders to be safer online citizens!

> **“THESE ARE CONCERNS [GEN Z HAS] BEEN DEALING WITH THEIR WHOLE LIVES!”**

UNRAVELING THREADS

Have you heard the news about the newest social media platform?

At the start of July 2023, Meta announced a brand new venture. In addition to Facebook and Instagram, the team behind the latter application has built a sort of mass-chat platform called Threads.

Sound intriguing? Before you jump into any new software or website, though, it's important to ask yourself: How cyber-safe is this?

120M USERS

Threads gained 100M users in the first week of their launch, and currently have 120M active members right now.

37% GEN Z

Threads has a greater percentage of Gen Z users age 18-24 than both X (formerly Twitter) and Instagram. Men seem to use it more than women.

Initially, people seemed ready to embrace Threads with the same eagerness as they did the virtual reality idea. 100M users signed up for this competitor to X (previously known as Twitter).

Despite the excitement, over half the users on Threads stopped using the app within the first month.

Some critics have noticed that Threads collects a lot of personal data; more so than other social media platforms do, anyway. That includes your...

- Browsing history
- Geolocation
- Search history
- Employment and union status
- Health information
- Race, ethnicity and sexual orientation

Additionally, you can deactivate your Threads profile once you make one...but it doesn't go away completely—unless you delete your whole Instagram too.

Then there are the ongoing privacy concerns: Since they became child companies of the same corporation, Instagram has long shared user data with Facebook and all their advertisers. Who's to say Threads won't encounter the same issue, and fan the flames even more? If they don't add Threads data to this same, massive database, then where does it go? Who can see that data?

It's not just about your data being sold to advertisers and sellers. Whenever new platforms come out, catfish flock to make fake profiles to phish or even spear-phish you. All of the social engineering attacks that you've learned about are just as much of a risk on Threads as they are anywhere else.

So, are you excited to jump onto the platform? Or do you think Meta has too much control over your online presence as it is?

That's up to you to decide!

Just do your research before jumping onto new trends. Take serious precautions when you sign up for new accounts; know who can access that data and how much of your activity they are able to track. The more you know about a website and what security risks could lie there, the better decisions you can make about your data's privacy!

"THREADS COLLECTS A LOT OF PERSONAL DATA; MORE SO THAN OTHER SOCIAL MEDIA PLATFORMS..."

“There was a second problem that was still not a technical problem... the project became classified. I couldn't work on it after having gone to all that trouble. I was considered a security risk, so I could not get a clearance.”

-GORDON GOULD

WHY DO WE HAVE CLEARANCE LEVELS?

Clearance levels help a company's cybersecurity by restricting access to sensitive information to those who have been vetted and deemed trustworthy. This helps to protect the information from unauthorized disclosure or misuse.

The level of clearance required for a particular position is determined by the sensitivity of the information that the position has access to. For example, a position that requires access to top-secret information would require a higher level of clearance than a position that only requires access to confidential information.

The clearance process typically involves a background check, which may include interviews with the applicant's friends, family, and former employers. The background check is designed to identify any potential security risks, such as criminal activity or financial problems.

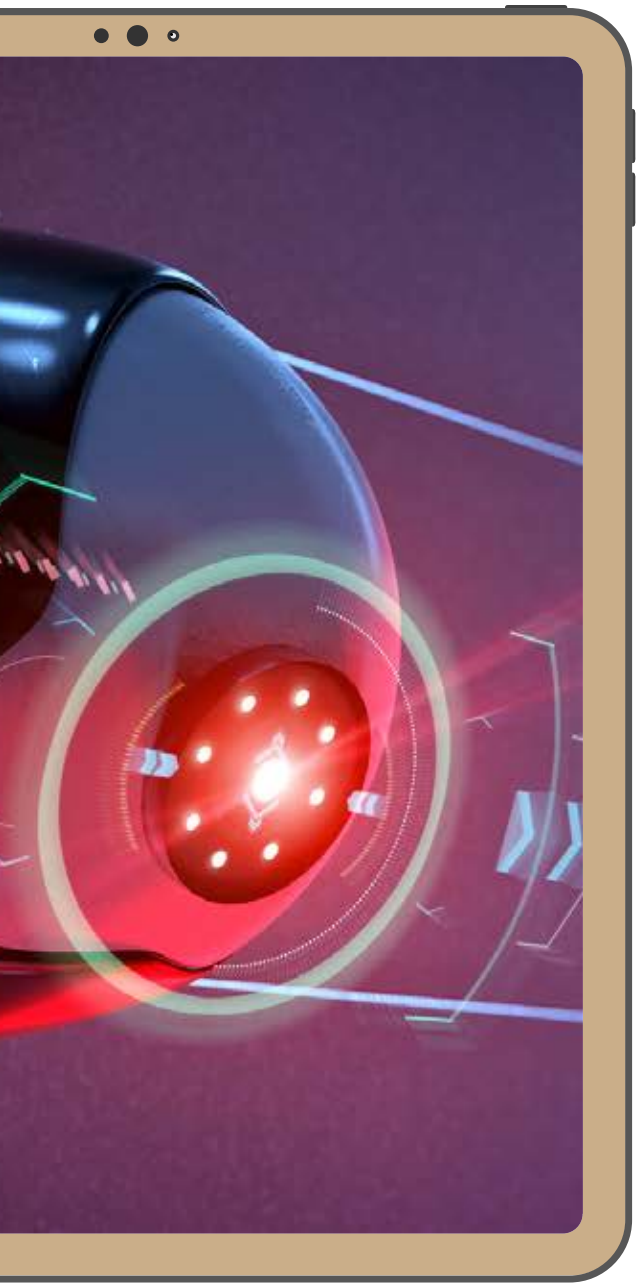
When you are granted security clearance, you are typically prohibited from disclosing that classified information.

Clearance levels...

✅ prevent unauthorized access to sensitive information.
✅ deter insider threats.
✅ identify and mitigate security risks.
✅ improve the overall security posture of the organization.

Clearance levels stop people from viewing sensitive documents and data, whether by accident or because they have something malicious in mind.

WHEN CLEARANCE IS BREACHED



No matter how hard we try, sometimes an insider threat just gets through. Whether it's a coworker accidentally sending confidential files to a junior staff member, or an intentional breach of the company's trust, clearance levels unfortunately don't keep out everyone!

- Individuals with security clearances should be properly trained on the security requirements that apply to them.
- Organizations should have strong security policies and procedures in place to protect classified information.
- Individuals should be vigilant about protecting classified information, and should report any suspicious activity to their security office.

IF IT HAPPENS TO YOU?

If you are found responsible for breaching your clearance level, you not only face them revoking or suspending your access to that information. You could lose your job, have difficulties finding a new one, and even be prosecuted and face penalty fees.

Take security clearances seriously! Your boss and the state sure do.

APPLICATION LISTS

There are all kinds of applications that you can, and might already have, installed on whatever device you're reading this on!

If it's a laptop or desktop computer, you might have programs like Microsoft Office, Spotify, Slack, and even games like Minecraft or the Sims. Meanwhile your phone may have apps downloaded like Apple Music or iMessage.

Unfortunately, not all applications are useful—or even safe. Legacy applications that are discontinued probably have all sorts of outdated defense systems that modern cybercriminals can slip past with modern technology. Some threat actors may try to covertly install malicious applications on your device to launch malware or ransomware.

Thankfully, your IT team knows how to guarantee only secure apps end up installed on your system. They can use tools called an **application whitelist** and an **application blacklist** to determine which specific apps and programs are safe to use, and that won't distract you or put the work network at risk.

9 OUT OF 80

The average mobile phone has 80 apps installed, but a study at BuildFire reveal that people only regularly use about 9, and visit around 30 each month.

GAMES

The most popularly downloaded type of app on both the Apple Store and Google Play Store are games, begetting more than 800M registered games across app stores.

3 HOURS

On average, people use their smartphones for more than three hours a day, mostly spending that time on their apps, according to a study by Insider Intelligence.

WHITELIST VS BLACKLIST

Application Whitelists	Application Blacklists
Takes a proactive approach to security	Takes a defensive approach to security
Only lets in *trusted*, positive applications	Blocks negative, unwanted application
Can be on the operating system, application or network level.	Can be on the operating system, application or network level.
Can be used to replace legacy applications with newer versions	Can disable compromised apps ASAP
Valuable tool for preventing malware	Valuable tool for preventing malware
Used to ensure users only use safe apps that won't distract them	Used to ensure users can't access dangerous or distracting applications

HOW TO REACH

CYBER COMPLIANCE

WHAT IS COMPLIANCE?

Cyber compliance is the process of ensuring that organizations adhere to laws, regulations, and standards related to the use of technology. It is an essential part of any organization's security strategy as it helps protect against cyber threats and data breaches!

If that's not a compelling enough reason, you could also be held liable in an audit if you are caught slacking on cybersecurity.

Cyber compliance ensures that an organization's systems and data are secure from cyber threats.

What does this involve?

- Assessing risks
- Developing policies and procedures
- Implementing security controls
- Monitoring changes in technology

These are just a few responsibilities that will help protect your systems against the ever-evolving landscape of cyber threats.

Compliance laws aren't here to wrap you up in red tape. They're meant to better protect your personally identifiable information (commonly known as PII), as well as anyone else's protected data entrusted to your company's care, and yours as a consequence.

By taking necessary steps to protect their systems and data, organizations can reduce the risk of breaches or other malicious activities!

DID YOU KNOW?

2/3 That's how many small- to medium-sized businesses go under after a data breach.

Source: National Cybersecurity Alliance

39 % of organizations cite compliance as a "significant challenge."

Source: Checkpoint Systems

66 % 2/3 of SMBs estimate that more spending is going toward compliance.

Source: CSO Online

137 That's how many countries have enacted some kind of data privacy legislation.

“Space in general gave us GPS. That’s not specifically NASA, but it’s investments in space.”

-Neil deGrasse Tyson

YOUR PHONE KNOWS EVERYWHERE YOU GO

GEOLOCATION

When you open your Maps app and it knows exactly what cross-street you're lost between, or switch on your GPS, or when you look up "attractions near me." How does your phone, or whichever device you're using, know where you are?

Geolocation. Tracking the global position system (GPS) via satellite is the most common, but that's not the only way. Cell towers that triangulate your location, WiFi networks, and even IP addresses also show your location.

We use geolocation all the time, to reacquire lost devices, navigate around unfamiliar cities, enable target marketing, and promote safety like when you share your location with friends.

TURNING IT OFF

If you have privacy concerns because of geolocation, such as having your movements tracked without your consent, then there are ways to protect yourself.

- Disabling location services on your device: This will prevent apps from accessing your location.
- Using a VPN: A VPN encrypts your traffic and routes it through a server in another location. This can make it more difficult for websites and apps to track your location.
- Being aware of the apps that are using your location: When you install an app, check the permissions that it requests. If an app doesn't need to know your location, don't allow it to access it.

GEOTAGGING & GEOFENCING

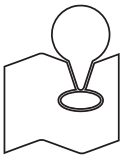
WHERE LOCATION SERVICES MEET PRIVACY

Whether you're checking in to someplace on Facebook, or browsing posts made from a specific location on TikTok or Instagram, you've probably come across geotags before —maybe you've even used a few!

As you can probably imagine, always letting the whole Internet know where you are can pose a risk to you—and to your data's privacy.

Geotagging involves embedding location information (such as latitude and longitude coordinates) into digital media files. These can be photos, videos and even social media posts.

At work, there's the additional risk of exposing the location of sensitive business activities to competitors and adversaries. Even other people in the organization may not have the clearance level necessary to possess that knowledge.



If they can find out more about that "metadata," malicious actors would be able to track your movements and habits, potentially posing physical dangers and making it easier to spear-phish you with the perfect scam. They might send you tailored messages referencing your recent locations or activities, making their phishing attempts more convincing. You don't want to give out too much information about your daily routines and whereabouts online!

That's why it's important to beware what metadata you're putting out into the world by accident, and who exactly can see that information—if they know where to look.

Check your settings and disable geotags, at least on individual posts that could expose private information. Even still, be careful what you post online; consider sharing content only with a close circle of trusted friends or family.

GEOFENCING TO THE RESCUE

Instead of simply tracking and saving where you are, geofencing uses GPS (Global Positioning System), RFID (Radio Frequency Identification), Wi-Fi, or cellular data to create a virtual boundary or perimeter around a physical location.

When a device, such as a smartphone, enters or exits this defined area, it triggers certain actions or notifications. Perhaps you can't clock in off-premises, or need to be in a certain secure area to access more confidential documents. You probably encounter geofencing every day at work, without even realizing it!

Geofencing is commonly used in applications like location-based marketing, fleet management and access control.

It can be used to enforce access control policies based on where you are physically located. For example, your organization might use geofencing to allow or restrict access to certain sensitive systems or data, based on the user's position. If you use some kind of time keeping system, they might prevent you from clocking in off-premises.

If a company operates in a region with strict data privacy laws, they might use geofencing to block users from transferring data to countries with less stringent regulations. This can ensure compliance with data protection laws!

If you work remotely all or even some of the time, then geofencing can help with secure mobile device management and flexible workplace policies. Your company might enforce security measures, such as requiring stronger authentication or encryption, when devices are used outside approved geographic areas/

Your IT experts might also use it to manage or restrict access to their internal network from specific geographic regions known for high levels of cybercrime or hacking, or use it to note suspicious internal activity.

MOBILE DEVICE MANAGEMENT

FOR WHEN YOU WORK REMOTELY

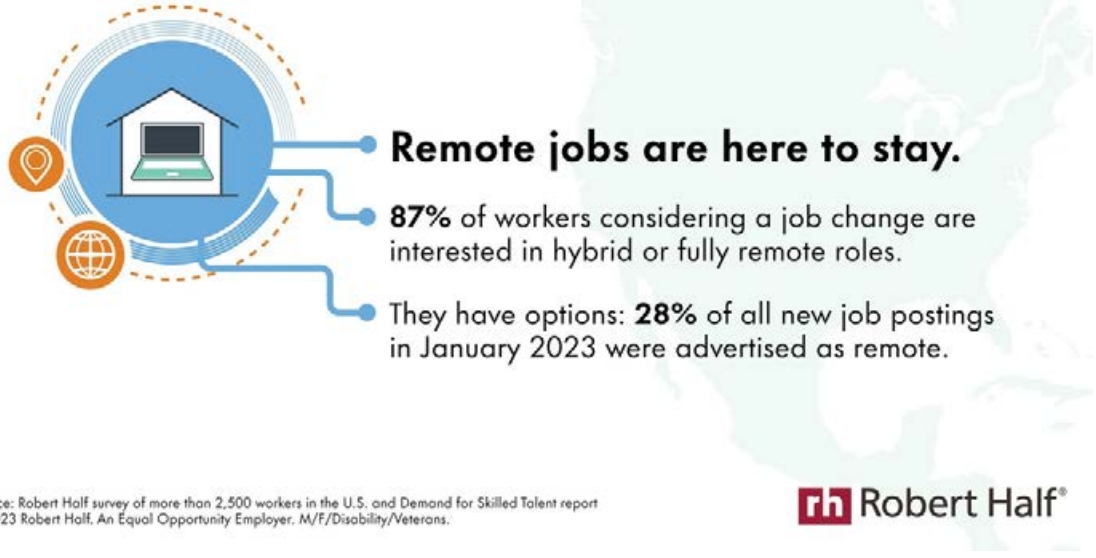
Have you ever checked your work email while on vacation with your tablet?

Maybe your job sends you to other states or even outside the country, sending along a company laptop with remote access software.

There are a ton of reasons why you might use devices that let you go online, and even access sensitive projects and work files from anywhere in the world (with WiFi, of course!). You should know, though, that your organization may enforce mobile device management policies when you log in outside of the office.

27% *of American workers are remote*

28% *of employees enjoy a hybrid schedule*



Multi-Factor authentication, encryption technology and remote data wiping software can all help prevent unauthorized third parties from logging in through the same remote access technology.

If your device is lost or stolen, MDM allows organizations to remotely lock and/or wipe the device, ensuring that sensitive data doesn't fall into the wrong hands. This is incredibly useful for management oversight, especially within organizations that regularly rely on mobile devices like a tablet.

It also lets YOU manage your personal devices with ease—if you lose your phone, you can go onto a computer to lock, wipe or search for it.

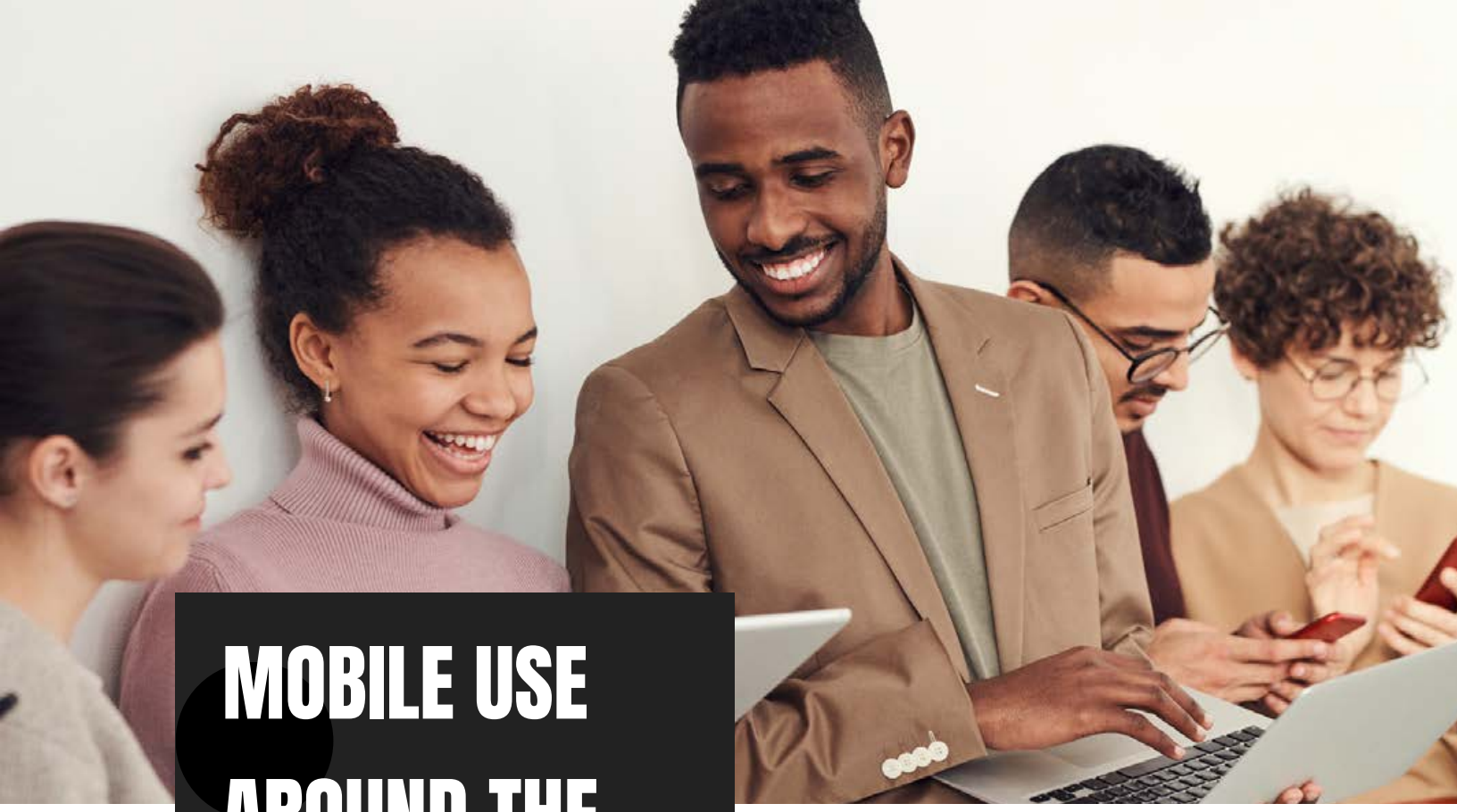
Meanwhile, depending on where you work and what you do, your organization may be beholden to certain regional privacy laws. They might enforce geofencing technology as one part of their overall solution to comply with regional legislations.

In this on-the-go, fast-paced world, we all use mobile devices like our phones, bluetooth players and smart technology. It's important that we can manage the security of our private data, even if we are physically away from the servers or remotely logging into the network. Modern MDM technology not only makes that possible, but it keeps us safe while we do it!

> "INCREDIBLY USEFUL FOR MANAGEMENT... WITHIN ORGANIZATIONS THAT REGULARLY RELY ON MOBILE DEVICES"

COMMON MOBILE DEVICES THAT YOUR ORGANIZATION MIGHT MANAGE:

- ***Smartphones:*** You might communicate with team members via app or text
- ***Tablets:*** Tablets offer the same advantages with a bigger screen.
- ***Laptops:*** Portable computers are easiest for consistent, remote work.
- ***Wearable tech:*** Be careful using your smart watch's received notifications!



MOBILE USE AROUND THE GLOBE

67% *of American workers are remote*

70% *of employees enjoy a hybrid schedule*

Source: CNBC

85% *of the world owns a smartphone*

ARE YOU READY FOR SMARTER REMOTE WORK?

MDM solutions can help to protect sensitive data on mobile devices by enforcing security policies and by giving IT administrators remote control over the company's mobile devices.

It also helps reduce IT costs by automating many of the tasks that are involved in managing mobile devices, and simultaneously helps employees be more productive by providing them with the tools and resources they need to work from anywhere.

If you are looking for a way to manage and secure your organization's mobile devices, then MDM is a smart solution!

COMPLETE GUIDE TO MULTI-FACTOR AUTHENTICATION

Why do security experts insist on using multi-factor authentication, which you may sometimes see referred to as two-factor authentication, so strictly and for every account?

MFA adds an extra layer of security to your accounts, making them much more difficult for attackers to compromise. Even if an attacker knows your password, they will not be able to log in to your account without also having access to your MFA factor.

Thankfully, many types of MFA require biometric identification, which means using something completely unique to your person—like a fingerprint or face ID.

OTHER KINDS OF MFA

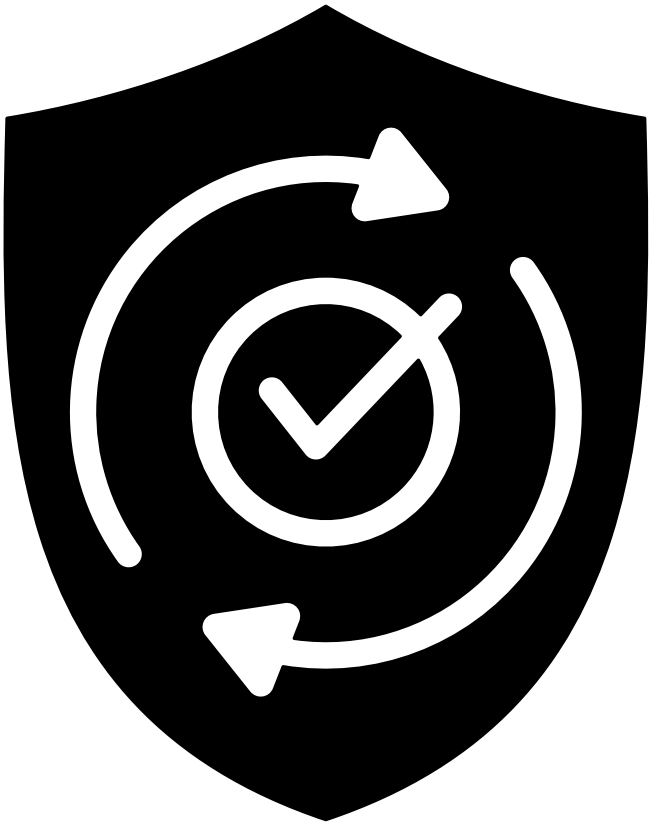
The strongest MFA factors are those that combine two or more different methods. For example, using both biometric ID and a one-time password, PIN or security question.

One-time passwords may be communicated via text, email or even phone call. Additionally, you might use a mobile app to generate a QR code or one-time password as well.

Other biometric identification that you might encounter, in addition to a fingerprint or facial recognition, are voice recognition and retina scans. Requiring these ID verifications can also protect physical assets, such as by requiring a handprint scan before allowing cleared personnel into a restricted area of the building.

IS MFA INFALIBLE?

In short: Of course not!



No technology is, for as long as cybercriminals exist, they will invent methods and technologies for thwarting even our best defenses! That includes multi-factor authentication.

- **MFA fatigue** involves barraging the victim with MFA requests until they accidentally approve one.
- **Man-in-the-middle attacks** intercept your communication with the service at hand. The bad actor spies on your activity to steal the one-time code.
- **SIM swapping** transfers your phone number to the threat actor's SIM cards, so they get the SMS codes instead.
- **Malware** can exploit MFA vulnerabilities to circumvent the entire MFA process.

So should we stop trusting MFA?

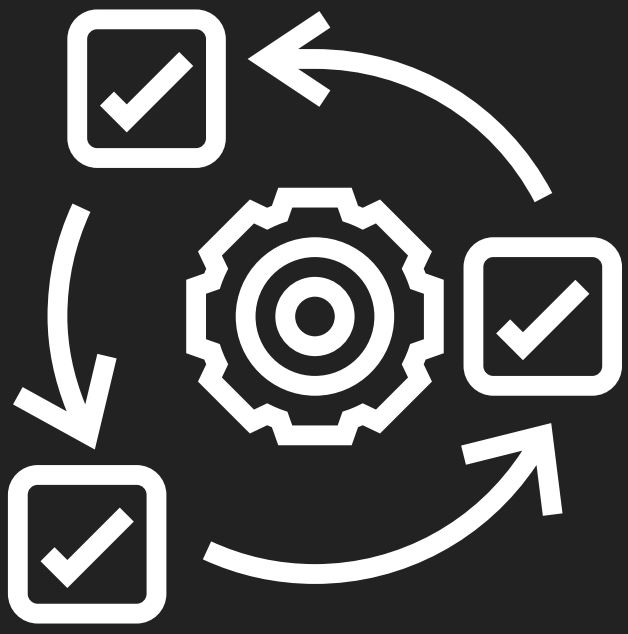
As previously stated, there's no such thing as 100% impenetrable technology. Nevertheless, MFA is much more difficult to falsify or break through by force than passwords alone.

Thus by using a strong MFA system and being aware of the different types of MFA bypass attacks, you can make it much more difficult for attackers to compromise your accounts.

Protect your accounts with the same ferocity with which hackers are trying to compromise them! MFA is a great tool to have on your side.

“Cybersecurity is not a product, it's a process.”

-Marcus Ranum



Did you know?

Some people get hacked on purpose. Yes, really!

No, we're not talking about insider threats that involve someone within the organization abusing their security privilege.

White hat hacking happens when companies actually hire someone to try and (legally) hack into their systems and data.

Then they get a detailed report that analyzes what went wrong, where their current security structure has weak points, and ideas about what to do next to prevent a real hack from penetrating the system as deeply.

- Most importantly, white hat hacking is **legal.**
- They have the intention of improving the security of the systems and network they're trying to break into.
- Use hacking techniques to test security systems and identify vulnerabilities

WHITE HAT HACKING

- They focus on understanding and strengthening security measures.
- They use a wide range of tools, like penetration testing, vulnerability scanning, and risk assessments.
- White hat hackers are often respected members of the cybersecurity community, and may receive recognition for their work.

- Black hat hacking is **illegal.**
- They want to sabotage your systems and network security to compromise your confidential data.
- Use hacking techniques to steal data, disrupt business and install malware

BLACK HAT HACKING

- Their actions can involve malware, phishing, and other malicious software.
- They use malicious techniques like malware, spam, phishing, social engineering and brute-force attacks.
- Black hat hackers are criminals, and will be apprehended if caught.

FACIAL RECOGNITION: FOR GOOD OR EVIL

- What is it?
- Is it used to hurt or help our personal privacy?

"KEEP YOUR IDENTITY, AND YOUR DATA, AS PRIVATE AS YOU WANT IT TO BE. OFTEN YOU CAN CHOOSE TO OPT IN OR OUT OF THIS SOFTWARE."

Facial recognition software is a technology that uses biometrics to identify people by their faces. It is becoming increasingly popular in security applications, such as access control, surveillance and fraud prevention.

- Identifies people who are not authorized to enter a restricted area.
- Tracks people's movements and identify suspicious activity or find missing persons.
- Prevents fraud, such as identity theft and credit card fraud.
- Improves customer experience, such as by allowing people to unlock their phones or log into their accounts with their faces.

How might this technology be used for evil? Perhaps you can already think of a few scenarios where you don't want your face logged into a database somewhere.

Other concerns with facial recognition software include...

- Used to invade people's privacy.
- Used to discriminate against people based on their appearance.
- Inaccurate, especially for people of color or with certain facial features.
- It can be hacked, which could allow criminals to access people's personal information.
- It can be used to create a surveillance state.

Do you share some, all or none of these concerns?

Did you know?

Almost 70% of Americans think facial recognition makes us all safer.

Over 70% of Americans think it would misinterpret employees' expressions.

Keep your identity, and your data, as private as YOU want it to be. Often you can choose to opt in or out of this software.

On the other hand, when you do choose to allow a device to log and remember your face, you should be sure the application takes the utmost care with privacy and includes state-of-the-art cybersecurity protection.

It takes careful consideration and research into what services you are trusting, however, there are ways to use facial recognition ethically and securely.

IS YOUR PERSONALLY IDENTIFIABLE INFORMATION ON

THE DARK WEB?

not with dark web monitoring software

DATA COLLECTION:

Dark web monitoring software needs to be able to collect data from the dark web, but they do it legally. This may involve methods like scanning dark web forums, marketplaces and chat rooms for your personally identifiable information.

DATA ANALYSIS:

Once the data is collected, it needs to be analyzed to identify any threats to the organization. Dark Web Monitoring technology may use methods such as machine learning and natural language processing to properly analyze the information it has collected.

ALERTING:

Once a threat is identified, the Dark Web Monitoring software needs to alert the organization so that they can take appropriate action. They may send automatic notifications to multiple people via email, SMS or push notification.

A security solution that includes Dark Web Monitoring can be a valuable tool for organizations of all sizes, as it can help them to identify and mitigate threats before they cause damage. The software can generate reports that provide insights into the threats out there, and simultaneously kickstart incident response protocol so that the team may address the issue more efficiently.

Overall, dark web monitoring software can help organizations to protect their data, their customers and their reputation too!

WHY WE USE DARK WEB MONITORING

- A company can use dark web monitoring software to identify whether any of their employees' credentials have been compromised in a data breach

- A financial institution might use dark web monitoring software to identify whether any of their customers' credit card numbers are being sold on the dark web

- Government agencies can use dark web monitoring software to identify whether any classified information has been leaked online

DID YOU KNOW?

5 FACTS ABOUT THE DARK WEB THAT MIGHT SHOCK YOU

Over 2.5M users visit the Dark Web every day.

According to Tor Metrics, their anonymous browsing software has reached over 2.7M daily users.

Anonymous browsers aren't illegal.

Despite what you may think, browsers like The Onion Router (known as Tor) are perfectly legal to download and use.

Malware is sold for as little as $5.

They can do hundreds of thousands of dollars in damages, but the cheapest malware, remote access trojans (RATs), start at five dollars on the Dark Web.

The largest dark market in 2022 had 1.3B users.

Hydra was the largest dark marketplace in the world until it was shut down by German and U.S. authorities.

The top 10 Dark Web forums have 80M messages.

PTSecurity found that over 7M topics, 8M users, and 80M posts comprise the 10 most active Dark Web forums.

CASE STUDY:

SHUTTING DOWN HYDRA

Who was Hydra?

Founded in 2015 by Russian hackers, Hydra quickly became the largest darknet marketplace in the world, and it was known for its wide variety of illicit goods and services, including drugs, weapons, stolen data, and hacking tools and kits.

Why was Hydra so successful?

This particular dark marketplace attracted so many underground users from all over the world, in part due to accessibility and ease of use. They also sold a wide variety of illicit goods and services, was operated by a sophisticated and experienced threat group, and built a strong reputation in the cybercriminal community over time.

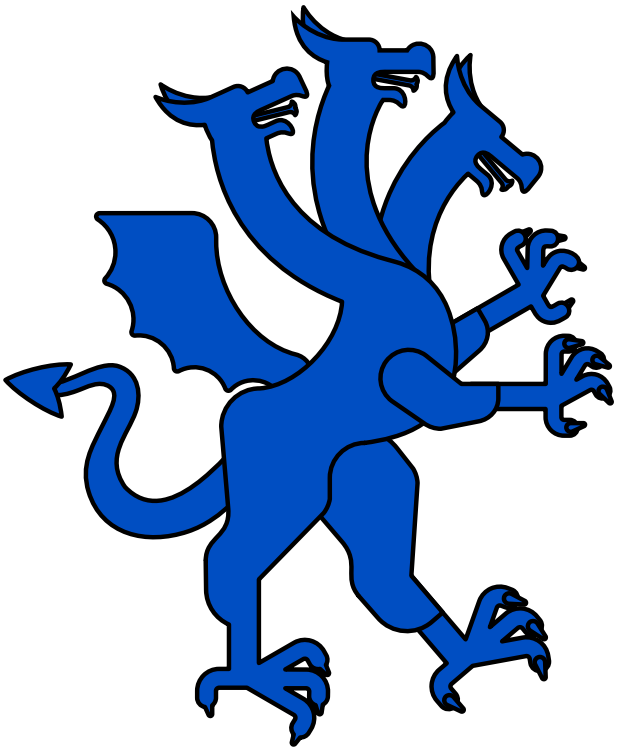
What happened to the dark marketplace?

Although other dark markets live on, Hydra was shut down in April 2022 by German law enforcement in cooperation with US law enforcement. The German Federal Criminal Police Office (BKA) seized Hydra's servers and cryptocurrency wallets containing $25M worth of bitcoin.

What does this mean for the Dark Marketplace?

The shutdown of Hydra was a major blow to the darknet marketplace ecosystem. However, darknet markets are resilient by nature, and new marketplaces have already emerged to take Hydra's place.

The shutdown of Hydra is a reminder that law enforcement agencies are working to combat darknet marketplaces. Darknet marketplaces are a complex problem, and there is no easy solution.



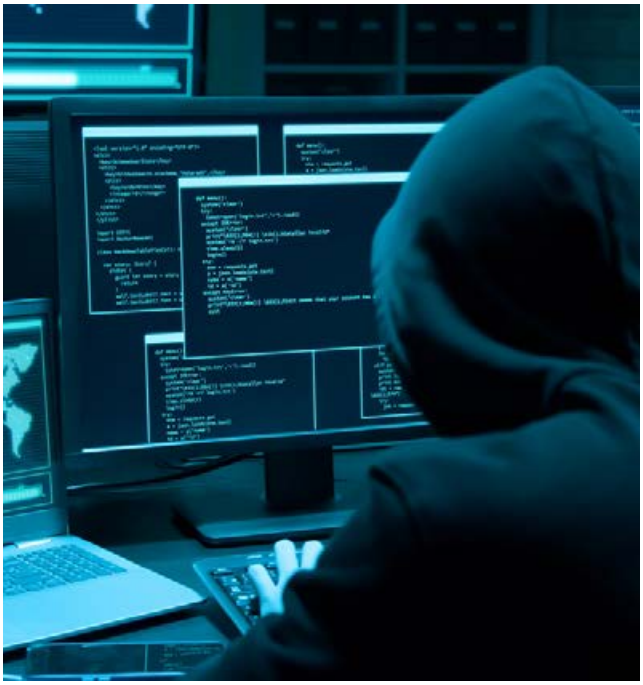
These days, cybercriminals don't have to be expert hackers themselves. Online, they can buy malware-as-a-service, ransomware kits and bundles of malicious code that even come with customer support to help walk them through how to execute the cyber attack.

That's why online marketplaces hosted on the darknet are so dangerous: Anyone with money and know-how can arm themselves with cyber-threats, and even get advice on how to use it. People review businesses and browse around just like legitimate online shopping.

Dark marketplaces are also used to commit...

- Money laundering
- Cryptocurrency fraud
- Theft of financial information
- Theft of PII and account credentials
- Hacking starter kits

Because it's so lucrative and in-demand by cyber-thieves, dark marketplaces are difficult to eradicate!



“The best security is obscurity, but that's not a viable strategy for the Internet.”

— Vint Cerf, “Father of the Internet”

SIGN ME UP FOR A FREE CYBER SECURITY RISK ASSESSMENT AND IT SYSTEMS CHECKUP

RAZZPRO.COM

Bringing you the cybersecurity news YOU need to stay up to date on the latest tricks and trends coming out of the dark web, as well as what security experts are developing to fight them.

SIGN UP NOW!

REVIEWS!

Liz Casella

★★★★★

Increased Uptime And Productivity While Decreasing Our IT Costs

The biggest benefit to using Razz Pro has been our improved uptime compared to previous IT vendors. They also helped to reduce our overall IT costs with their VoIP phone solution.

Director Liz Casella LLC

Jordan Kerner

★★★★★

Helped us be safe on the internet

Razz Pro added a great firewall. They installed a system that automatically backs us up throughout the day. Razz Pro is an essential service for our film production company!

Producer/Owner
The Kerner Entertainment Company

Alison Grabell

★★★★★

Use Or Choose Another IT Firm At Your Own Peril!

Razz Pro is knowledgeable, responsive and they are incredible IT problem solvers. They understand us from a business perspective and the world in which we work, not only from a technology view.

Founder MarkStarLaw

Rick Newcombe

★★★★★

Nothing but positive feedback from our employees!

Our servers and computers are monitored by Razz Pro remotely. We have been able to avoid problems like we had in the past, when those devices would go down.

Business Owner of Creators Syndicate

REAL SATISFACTION GUARANTEED

CYBERSECURITY YOU CAN TRUST

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

Call us today at **310-695-2199** and let us help you wrap a security blanket around your business.