OCTOBER 2024

ISSUE NO. 43

THE DIGITAL DOWNLOAD

ADVANCED PERSISTENT THREATS

page 8

FEATURING: TIM NYBERG, FOUNDER OF THE MACGUYS+

page 12

KEEPING TRACK OF DATA PRIVACY

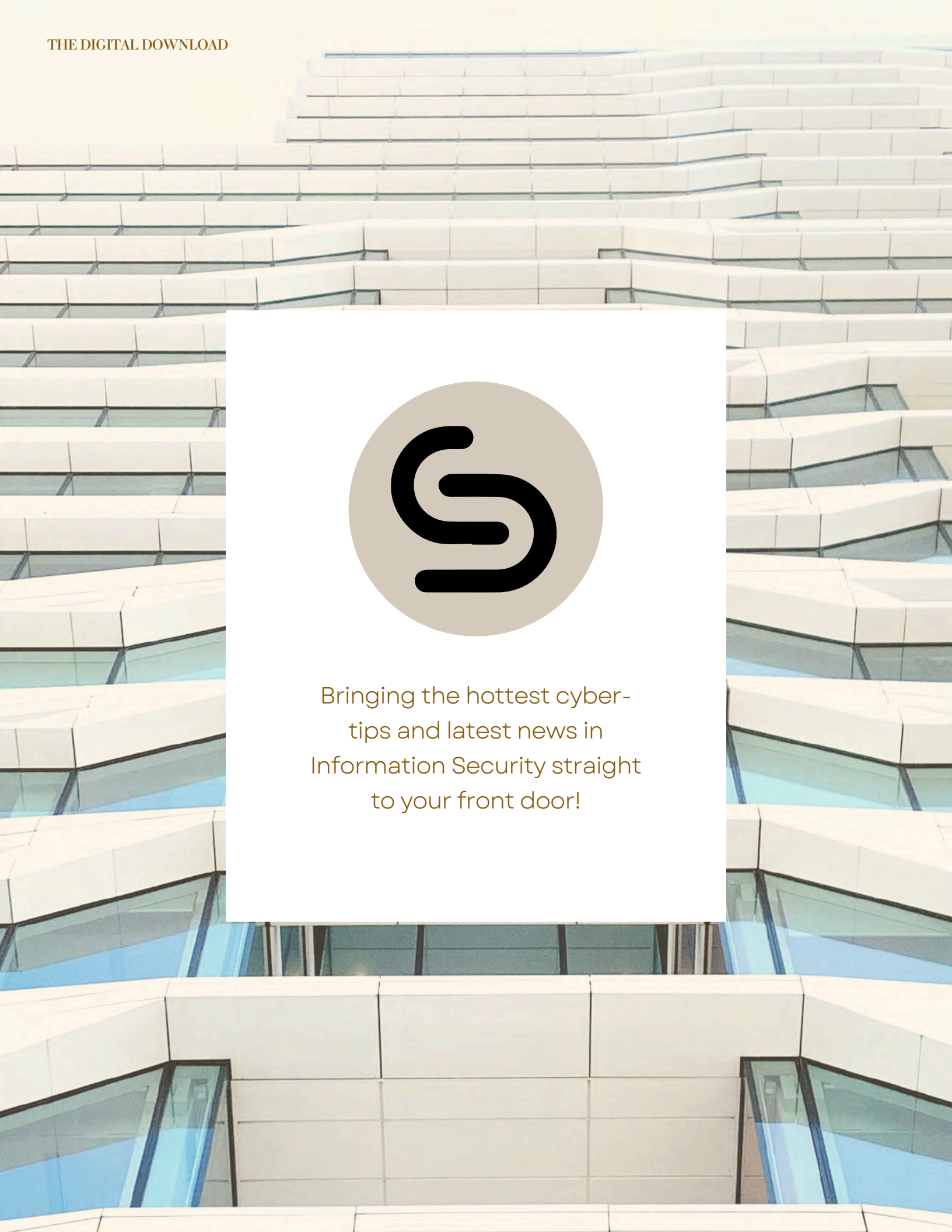
page 24

STRONG ENOUGH FOR TYPOSQUATS?

page 28

360°

coverage, all year round



Bringing the hottest cyber-tips and latest news in Information Security straight to your front door!

EDITOR'S NOTE

The team behind The Digital Download want to thank you for your subscription. We put in the hard work to create this magazine so that you can more easily stay up to date with the most relevant trends, ideas and news in the cybersecurity industry. Not only that, but we interview REAL INDUSTRY EXPERTS to get the scoop from the brightest minds in the game.

We aim to cut through the confusion of technical jargon so that anybody, regardless of whether they have any background in information security, can understand it.

It all comes back to our core mission: To make YOU as cyber-safe as you can be!

TABLE OF CONTENTS

AS THE WORLD IS INCREASINGLY INTERCONNECTED, EVERYONE SHARES THE RESPONSIBILITY OF SECURING CYBERSPACE.

-Newton Lee

3 PHISHING TRICKS YOU MIGHT NOT HAVE THOUGHT ABOUT

1. Spoofed numbers and domains

Imagine this: Your phone rings, and when you take it out of your pocket...the caller ID says U.S. Border & Customs Patrol! Even worse, when you pick up, they say that there's tons of illegal imported goods in *your name*, and they want your financial information ASAP to prove that you're not a smuggler.

Wait right there...the government doesn't ask you to send money over the phone!

That's right, just because a phone number *appears* to match an official agency—or if an email's domain seems to be from a legitimate source—remember that cybercriminals can spoof numbers, caller ID and email addresses to say whatever they want!

Whenever someone urges you to act quickly, and especially if they request money, *slow down!* It's probably a scam.

2. Different alphabets

Alpha, theta. delta, gamma...no, we're not talking about Greek Life. If you've ever taken an advanced math class, then you might recognize these better as symbols: α. θ, δ, γ...

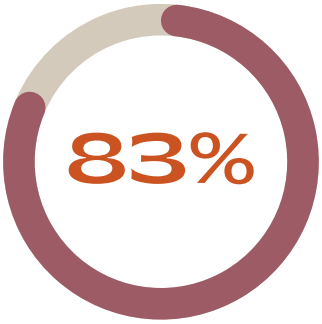
Then there's the host of other languages that exist! Not all of them use the same letters and symbols as us; but many may be close...Would you notice Google.com versus Googlè.com? Maybe, but some people will be tricked into thinking it's a familiar, trusted domain at just a glance!

3. Persistence and Fatigue

Cybercriminals don't have to trick you over and over and over again; rather, they merely have to break into your systems or accounts once. Once they learn your password, they know it until you change it. If they can bypass your defenses and breach the network, they could stay there until you kick them out and reinforce the system.

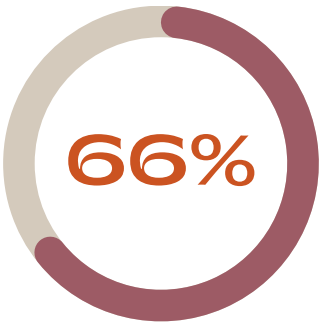
Thus *MFA fatigue* can easily undo the most careful system user if they have just one day of poor concentration. In this attack, threat actors send multi-factor authentication requests until you accidentally approve one of them.

Similarly, *advanced persistent threats* rely on waiting out the user. Instead of trying to wear you down, these kinds of cyber-threats lay in wait, without their victims' knowledge, to siphon tons of data from their system over time.



Out of all the U.K. businesses that suffered a cyberattack last year, 83% report that the incident was related to phishing.

Source: UK Government's Cyber Security Breaches Survey 2022



That's how many breaches are caused by spear-phishing emails–despite them making up less than 1% of all messages.

Source: Barracuda Networks

ADVANCED PERSISTENT THREATS

Advanced persistent threats: have you heard of them before?

Known commonly as APT, these threats encompass any sophisticated, long-term, and undetected hack on your system. By remaining secretive, these bad actors are able to steal sensitive data over a prolonged period of time.

APT attacks are typically carried out by highly skilled, motivated and organized threat actors that operate in groups.

They often target specific organizations or industries for long-term espionage or sabotage, and use sophisticated tools to evade traditional security controls. That's why advanced protection is so important against advanced persistent threats!

Moreover, these groups are known for being quite patient and persistent, so they can remain in a network for months or even YEARS without detection!

Once they have access to a network, APT attackers have something of a carte blanche; they can move laterally within the network, escalate their privileges and steal sensitive data with ease.

So how exactly do APT threat groups gain access to their target networks?

Much like any other cybercriminal scheme, APT groups use spear phishing, social engineering and exploitable software vulnerabilities to gain initial access to their victim's systems.

Some of the most well-known APT threat groups include:

- APT28 (Fancy Bear)
- APT29 (Cozy Bear)
- APT41 (Winnti Group)
- APT32 (OceanLotus)
- APT36 (Charming Kitten)
- APT40 (Periscope Group)
- APT50 (Lazarus Group)

So...how can YOU protect your data from APTs?

CASE STUDY: RED CROSS SCAM

would you recognize this as an attempted cyber-attack?

Think about it: The Red Cross represents charity and the kind of goodwill that tempts people into helping their community. This is especially true after a natural disaster and other major events that require the Red Cross's help.

So in many ways, it makes sense that a threat actor who relies on social engineering techniques would try to capitalize on the Red Cross's good reputation to trick victims into sharing personal information.

In late September 2023, an *advanced persistent threat* (APT) group deemed "AtlasCross" sent their victim pool an attachment called Blood Drive September 2023.docm

Inside there lay a file titled Become a Blood Donor, which secretly kickstarted a malware .PKG in the background. Just like that, the victims' desire to do good backfires on their private data.

AtlasAgent, as the trojan was dubbed, would then begin stealing user information and system data.

Threat actors often use "masks" of large organizations to increase their likely victim pool; in this case, the lure is doubled by using a charitable organization as a cover. Phishing scams often rely on pivotal emotions like goodwill, guilt, pity and fear to engender a sense of timeliness regarding their proposal.

This is why it is so critical to beware attachments, even when you THINK it's coming from somebody that you trust.

Whenever possible, go through the organization's main site in a separate tab to ensure you are communicating with the real team on secure channels. NEVER send private information through insecure channels!

It's not only scammers masquerading as the Red Cross that you have to worry about. Phishers LOVE to use big organizations to widen their net of potential victims.

The brands most commonly used as cybercriminal "masks" are:

1. Microsoft ranks first, making up 29% of phishing schemes.
2. Google comes second, accounting for 19.5% of phishing masks.
3. Apple ranks at 5.2%
4. Wells Fargo is impersonated in 4.2% of phishing emails.
5. Amazon accounts for 4% of phishing masks.

Source: Check Point Brand Phishing Report for Q2 2023 Research

How can YOU avoid phishing scams?

- **Be suspicious of any email that asks for personal information.** Legitimate companies will not ask for your personal information via email.
- **Hover over links before you click on them.** This will show you the actual URL that the link goes to. If the URL does not match the website that the link is supposed to go to, do not click on it.
- **Be careful about opening attachments.** Only open attachments from people you know and trust. If you are unsure about an attachment, do not open it.
- **Keep your software up to date.** Software updates often include security patches that can help protect you from phishing attacks.

If you are unsure about an email or attachment, it is always best to err on the side of caution! Delete or verify the sender before doing anything else.

CAN YOU WITHSTAND BAD ACTORS' WORST WEAPONS?

TIMOTHY NYBERG

FOUNDER OF THE MACGUYS+

FEATURING TIM NYBERG

No matter where you live and work, there are probably some cybersecurity laws that apply to you. Maybe you handle health information at work, or frequently contract with the government.

Whatever your job, when you're handling, managing or even simply communicating other people's private information, that makes YOU responsible for keeping that data safe.

How can you be sure that you're effectively managing the *personally identifiable information* and other confidential data on your systems?

To find that out, we reached out to cybersecurity expert Tim Nyberg, founder and CEO of The MacGuys+, to answer our toughest questions!

with Tim Nyberg,
Founder of The MacGuys+

BIGGEST THREAT TO PII

Is Your Personally Identifiable Information Safe From Thieves?

Whether you're concerned about protecting your own personal data, or managing other people's sensitive information (like work clients and company secrets), you can guarantee that cybercriminals are trying to find a way to steal it.

The first and most important step to defending your PII? Understanding the most significant and dangerous threats against that private data!

That's why we turned to our featured expert, CEO and Founder of The MacGuys+, Mr. Tim Nyberg.

First and foremost, he warns us to watch out for phishing.

"***Phishing*** is a prevalent threat where ***attackers trick individuals into providing sensitive information through fake emails, websites, or text messages***. These attacks can lead to unauthorized access to PII."

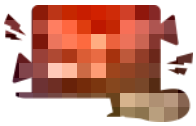
If you see a suspicious message, it's best to slow down and verify the sender's email address and requests. Don't click links or attachments you aren't expecting to receive; and ensure the grammar and spellings are correct, sounds local, and doesn't pressure you into doing anything hasty.

When you click on a false link or download an malicious attachment, Mr. Nyberg explained, it could immediately infect your device with ***malware*** or ***ransomware,*** without you knowing until it's too late.

"Malware and ransomware can ***infect devices, steal PII, or lock data until a ransom is paid,***" Mr. Nyberg explained. "Macs, while safer than PCs, are not immune to sophisticated malware attacks. Even organizations using Macs need robust security measures to protect against breaches."

Unfortunately, ANY unauthorized access to systems storing PII can result in a large-scale data breach. That's one of the many reasons that even YOU must be vigilant at work, because it's not just about keeping outsiders away...

Sometimes, the call really is coming from inside the house!



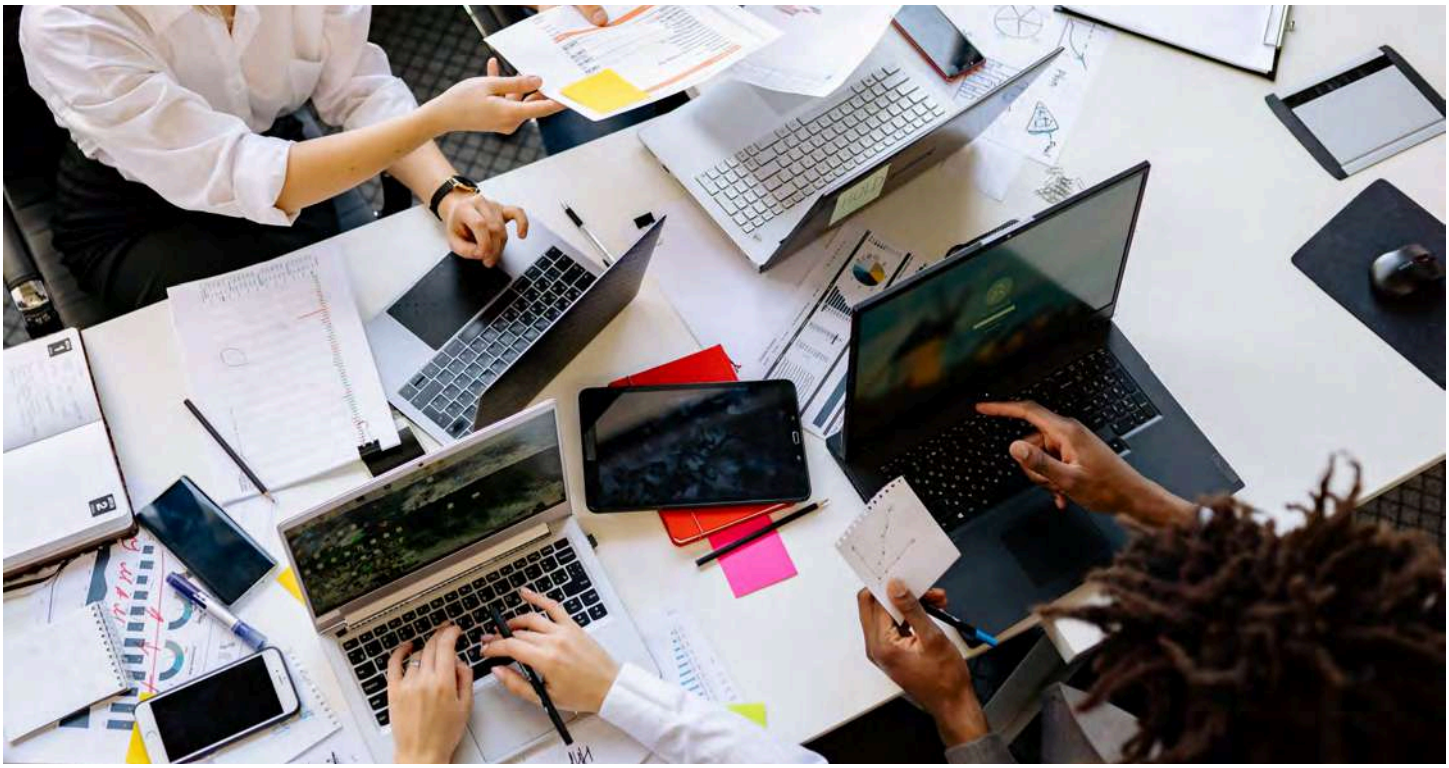
"Insiders with access to PII can intentionally or unintentionally leak information," said Mr. Nyberg. In this case, that means anyone who can legitimately enter the premises (or network) including employees, third party vendors or stockholders. "Proper access controls and monitoring are essential to mitigate this risk."

Think about it: You probably don't have free reign to go through your supervisor's office or confidential files.

Just as you have to abide the places you can go (online and offline), so does everybody else! If you see someone lurking in a place they shouldn't be, report the suspicious behavior.

Insiders don't always act out malice. In fact, attackers can manipulate individuals into divulging PII through various social engineering tactics.

"Education, training, and awareness are key to preventing such attacks," cautions Mr. Nyberg.



The complex world of cyber-threats and cyber-defense starts to get even more complicated when we mix in remote working conditions.

Whether it's working with someone who lives across the world, or simply logging in from a coffee shop on the other side of town, not everyone working on the company network is actually *in* the office.

Thus, it's important to understand that "using public or unsecured Wi-Fi networks can expose PII to interception by attackers," our visiting expert reminded us. "Encrypting connections and using VPNs can help protect data."

Secure work environments should include encrypted ***virtual private networks*** that allow you to access company information without compromising your connection. Even if someone spies on your communications, they'll only find scrambled tokens that they cannot unencrypt without the proper key (in other words, your password or biometric identification).

With these protections in place, our main concern then becomes what can happen if cybercriminals can *access* our accounts, and thereby see all of your encrypted and hidden files because they have the key (i.e. your credentials).

That was the driving factor behind expert Mr. Nyberg's dual warning and advice:

"Weak passwords or the lack of multi-factor authentication make it easier for attackers to gain unauthorized access to accounts and PII."

Keeping software and systems updated is another crucial factor for safeguarding your data.

"***Vulnerabilities in outdated software can be exploited*** to access PII," Mr. Nyberg explained. "This includes knowing which updates to run and which ones to hold off on. In many cases, ***big OS updates should be approached with caution***, so as not to break other services and hardware connections."

Protecting Yourself from Threats to Your PII

In this day and age of rapidly evolving technology, there's no doubt that you will inevitably encounter some kind of cyber-threat or convincing scam...or even worse, a full-on security breach!

"Implementing strong security measures, including ***encryption, regular updates, strong authentication, and user education***, is critical in mitigating these threats," our visiting expert stated. "For more specialized support, especially in a Mac environment, leveraging tools like iCloud Keychain for secure password management and staying vigilant against emerging threats are recommended."

How can you most effectively protect ***Personally Identifiable Information (PII)*** that is safeguarded and managed in your Mac-based organization?

Here's what our Mac expert, Tim Nyberg, recommended that we consider:

1. Strong, Unique Passwords and Multi-Factor Authentication (MFA)

Employ a robust password manager to generate and store complex passwords. This ensures passwords are *unique* and *securely managed.*

Then, utilize MFA to add an extra layer of security. This makes it harder for unauthorized individuals to access accounts!

2. Regular Software Updates

Ensure macOS and all applications are always up-to-date, because regular updates often include vital security patches.

Turning on automatic updates reduces the risk of forgetting manual updates.

3. Secure Networks

Use strong encryption for private Wi-Fi networks, and keep router firmware updated. Avoid accessing sensitive information over public Wi-Fi.

Use VPNs *(virtual private networks)* to encrypt internet traffic, which is especially important for remote work. Consider shutting down Wi-Fi after hours, so someone can't sneak on while the office is clear.

4, Data Encryption

Enable encryption features like FileVault to protect data on Mac devices.

Then, regularly ensure backups are encrypted to protect data even in storage.

5. Employee Training and Awareness

Train employees to recognize phishing attempts and other social engineering attacks.

Establish and enforce clear security policies for handling PII and have a security-minded culture at your business.

6. Access Controls

Limit access to PII based on the principle of least privilege. Only authorized personnel should have access to sensitive information.

Use secure methods for sharing sensitive information, like encrypted email and messaging services or secure cloud storage.

7. Regular Security Audits

Regular security audits help identify and address potential vulnerabilities.

Have a plan in place to respond to data breaches or security incidents quickly.

8. Backup and Disaster Recovery

Ensure critical data is backed up regularly.

Maintain a Disaster Recovery Plan to ensure business continuity in case of data loss or other emergencies.

By focusing on these areas, you can significantly enhance the protection of PII and reduce the risk of common threats, even with limited IT resources!

Our visiting expert, Mr. Nyberg, had this to say about the overall most effective way protecting your PII from common mistakes and threats.

“Keeping up with the latest security practices and leveraging built-in Apple tools will help maintain a strong data security posture,” he assured us.

Many times, breaches are incredibly difficult to recover from, particularly for small businesses.

Mr. Nyberg explains:

“Enforcement agencies like the FBI often have limited resources and may not respond to incidents ***with losses under $150k.*** This threshold is quite high for most small business clients. Therefore, it's essential to have good cyber insurance and reliable backups in place. Along with following best practices such as strong password management, regular updates, and secure networks, these measures can provide crucial protection and aid in recovery if a breach occurs.”

HOW THE MACGUYS+ CAN HELP YOU

A good MSP doesn’t just stop cyber-threats from happening...they also jump into action when an incident occurs!

Here is how The MacGuys+ handles trouble like this.

“Just before I onboarded a new client, they experienced a significant data breach due to a social engineering scam. They received a call that appeared to be from their bank, requesting updated information. The client, in a hurry, provided the requested details, believing the call to be legitimate. ***Within five minutes, $64k was withdrawn from their business banking account.”***

“After bringing this client onboard, we took several steps to secure their information. First, we brought their passwords and data under control by using a reliable password manager. Then, we initiated training sessions to educate the team on identifying and preventing social engineering scams like the one they encountered. By implementing these measures, we enhanced their security and helped prevent future incidents.”

Security Awareness On the Horizon

So what cyber-threats do YOU most need to consider? Remember, it all depends on your position and industry; the CEO of a retail franchise may be sought out to extort company funds, whereas a healthcare worker would be more likely to encounter spear-phishing campaigns aimed at stealing patient data.

Nevertheless, certain threats are more abundant across the board. For example, ransomware has been troubling every industry indiscriminately.

Did you know? In the last year, nearly 2,000 ransomware attacks have been unleashed throughout the U.S., Germany, France and the U.K according to a report by Malwarebytes Threat Intelligence!

When asked if there was any parting wisdom that they would recommend for remaining more cybersecure and cyber-aware in the coming year?

“If I could include one piece of advice in every single system user's Security Awareness Training in 2024, especially for small businesses or remote users,” said Mr. Tim Nyberg, “it would be: ***Implement and regularly update multi-factor authentication (MFA) for all accounts***."

Let’s dive into this one last nugget of insight before we let the Founder and CEO of The MacGuys+ go.

Why is multi-factor authentication so crucial?

We had Founder and CEO of The MacGuys+, Mr. Tim Nyberg, break it down for us! Here’s what he had to say about the importance of MFA.

- **Enhanced security:** MFA adds an extra layer of protection beyond just passwords. Even if a password is compromised, unauthorized access can still be prevented.

- **Protection Against Phishing:** MFA helps defend against phishing attacks, which remain a significant threat. If a user accidentally provides their credentials to a phishing site, the additional authentication step can stop the attacker.
- **Compatibility with Apple Ecosystem:** Apple devices support various MFA methods, including hardware tokens, authentication apps, and biometrics like Face ID and Touch ID. That makes it easier for Mac users to adopt and use MFA!

“MFA ADDS AN EXTRA LAYER OF PROTECT-ION”

Are you ready to take the plunge and implement MFA on your accounts? Mr. Nyberg also gave us the inside scoop on how to use MFA most effectively.

For starters, avoid one-time passwords to your SMS or email.

“Instead, utilize apps like Google Authenticator or Authy instead of SMS-based MFA, which can be vulnerable to SIM swapping attacks,” said Mr. Nyberg. “We also recommend using 1Password as a password manager, which can store and process the 2FA codes for you very efficiently and share that between your devices.”

- **Enable Built-In Apple Features:** Leverage Apple's built-in security features, like iCloud Keychain, for password management and MFA setup. Ensure that users know how to enable and use these features effectively.
- **Regular Updates and Reviews:** Make sure that MFA settings are reviewed and updated regularly. This includes updating contact methods and ensuring backup codes are stored securely.

Now, you may be wondering: *Why does this matter to me?*

The reality is that MFA doesn't just benefit your workplace...it also protects remote users and your personal systems, too!

"MFA significantly reduces the likelihood of unauthorized access, protecting sensitive business data and personal information," Mr. Nyberg explained to us. "Clients and partners are more likely to trust a business that demonstrates strong security practices."

There are also legal obligations to consider. MFA "helps meet regulatory requirements and industry standards that mandate the use of MFA," our visiting expert explained.

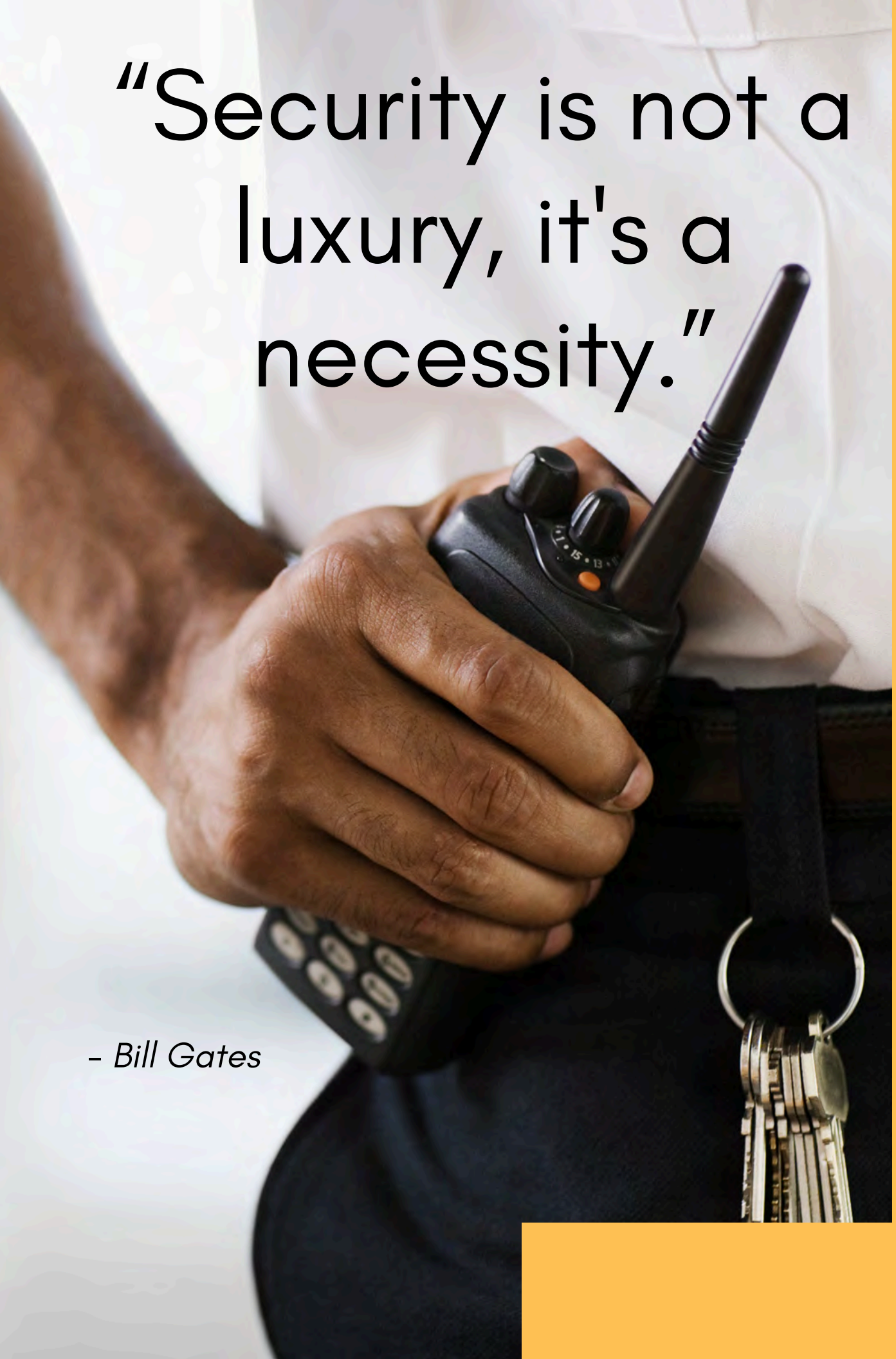
The importance of MFA isn't an over-exaggeration. It has helped solve REAL problems for The MacGuys+ and the businesses they service.

"One of my clients, a small business with remote employees, experienced a phishing attack where an employee's credentials were compromised," Mr. Nyberg disclosed. "However, because MFA was in place, the attacker couldn't gain access to the system. This incident underscored the effectiveness of MFA and reinforced the importance of ongoing security awareness training!"

Encouraging every user to adopt and understand the importance of MFA can significantly bolster your organization's security posture, especially in a landscape where remote work and digital threats are on the rise.

When asked for one last snippet of advice before he departs, the CEO and Founder of TheMacGuys+ had this to say:

"Multi-factor authentication is your first line of defense in an interconnected world!"


"Security is not a luxury, it's a necessity."
- Bill Gates

Some people worry about the potential for artificial intelligence to become too powerful and pose a threat to humanity. Others worry about the depletion of resources and the pollution caused by technology.

Technology has also improved our lives in many ways, from making it easier to communicate and stay connected with loved ones to making it easier to access information and services.

KEEPING TRACK OF DATA PRIVACY

Technology has also made it easier than ever for companies and governments to collect and track our personal data. This has led to many concerns about privacy and the potential for abuse.

When it comes to modern privacy, that includes who can track and sell what we do on the world wide web.

Now, you may wonder why this is beneficial to companies, anyway. Do they really need to know that you checked your blog eight times today?

If you ask these sites' marketing teams, they would give you a resounding YES!

When a website (or application, etc.) collects data about you — such as pages viewed, searches performed and products purchased — all of those cookies and pixels can be used to target ads directly to and for you. These metrics may also factor into negotiations with advertisers on their website;; ever notice how Facebook's sidebar ads can show nearby products that you've Google searched before?

Your Internet service provider (ISP) may also track your online activity, including the websites you visit and the files you download. It may help with troubleshooting and complying with police.

Social media tracks data, for example, TikTok measuring how long you linger on certain videos to develop their algorithm, or Instagram using geolocation to provide more relevant searches.

The government can also collect Internet data to assist with national security, legal investigations, and even tax collection!

Of course, there are local and federal laws all over the world dedicated to better protecting citizens' private data, from bad actors and advertisers alike!

How much of YOUR data is being tracked right now?

PROTECTING DATA

- Use a privacy-focused browser, such as Brave and DuckDuckGo, to block trackers and other data collection technologies.
- A VPN encrypts your traffic and hides your IP address, making it more difficult to track you.
- Only share information with trusted people and sources.
- Regularly review your privacy settings on websites and apps!

Keeping the Lid on Your Computer's Cookie Jar

When we talk about Internet "cookies," how much do you understand about what these little bites of data mean?

Cookies are simply text files stored in your browser's search history. They are not inherently malicious nor benign; although like anything technology-related, they can be *used* for good or bad.

So, how can you stop persistent companies and threat actors from taking a bite out of your cookies?

- Only accept cookies from trusted websites.
- Use a VPN to encrypt your traffic and hide your IP address.
- Regularly review your cookie settings. and disable or delete them in your browser settings.
- Keep your operating system up to date, and software updates often include security patches that can help to protect you from malicious cookies.

Cybercriminals can use cookies to steal personal information, track users' online activity and spread malware.

You should remember, though, that cookies can also be used to improve cybersecurity. For example, websites can use them to authenticate users and prevent unauthorized access to accounts. Cookies can also be used to prevent fraud and other threats.

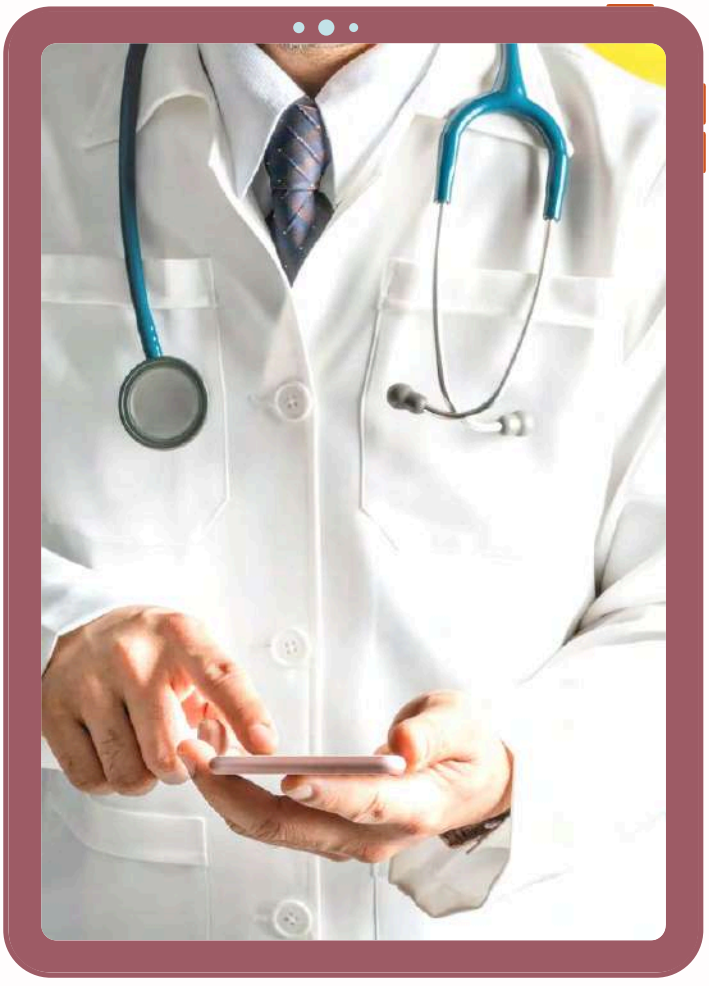
Cookies are neither good nor bad. It's about what you do with them!

Case Study: CVS Pharmacy

May 2021

We all do our best to avoid using suspicious, unsecured websites...especially if we plan to insert personal information, like our credit cards, birthdays and even private health data!

Unfortunately, that doesn't mean we're invulnerable to security threats. CVS and their customers found this out in 2021, when hackers injected malicious code into a CVS web page. When customers visited the page, the code was executed and their cookies were stolen — *even though* it was a website they had accessed a hundred times before!



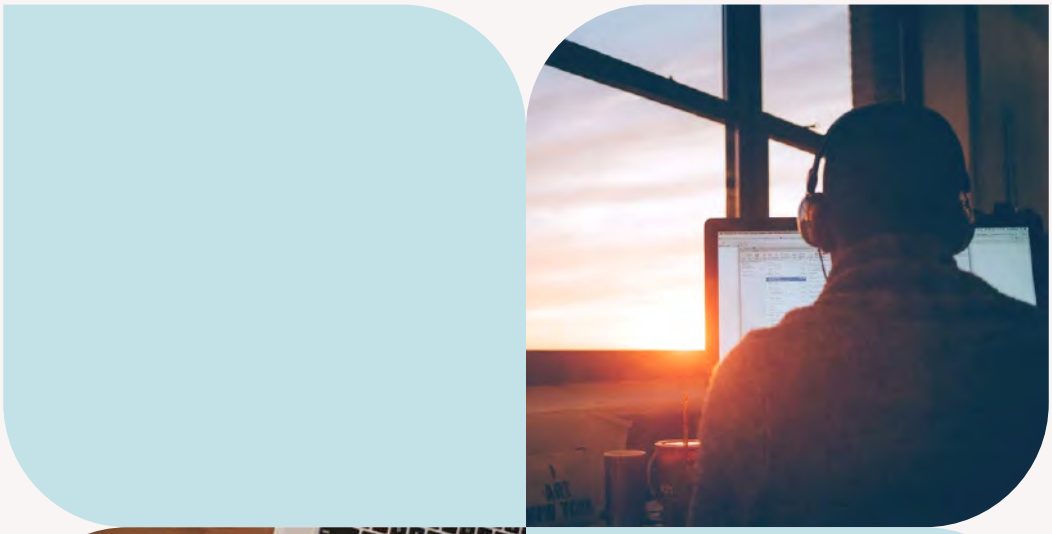
The hackers then used the stolen cookies to access customer accounts and steal personal information, including names, addresses, phone numbers and email addresses.

CVS discovered the attack in June 2021 and took steps to mitigate the damage, including notifying affected customers and changing their passwords. The company also launched an investigation into the attack with the help of law enforcement.

The hackers then used the stolen cookies to access customer accounts and steal personal information, including names, addresses, phone numbers and email addresses.

CVS discovered the attack in June 2021 and took steps to mitigate the damage, including notifying affected customers and changing their passwords. The company also launched an investigation into the attack with the help of law enforcement.

It just goes to show that even trusted websites can be compromised...and you'll be the one regretting it!



STRONG ENOUGH FOR TYPOSQUATS?

Typos are usually small mistakes you make when you're writing on your phone or computer. "Fat fingers" are responsible for writing "teh" instead of "the" and accidentally ending a sentence in "1" instead of "!". Unlike a simple typo when you're messaging your friends, though, ***typosquatting*** is much more sinister.

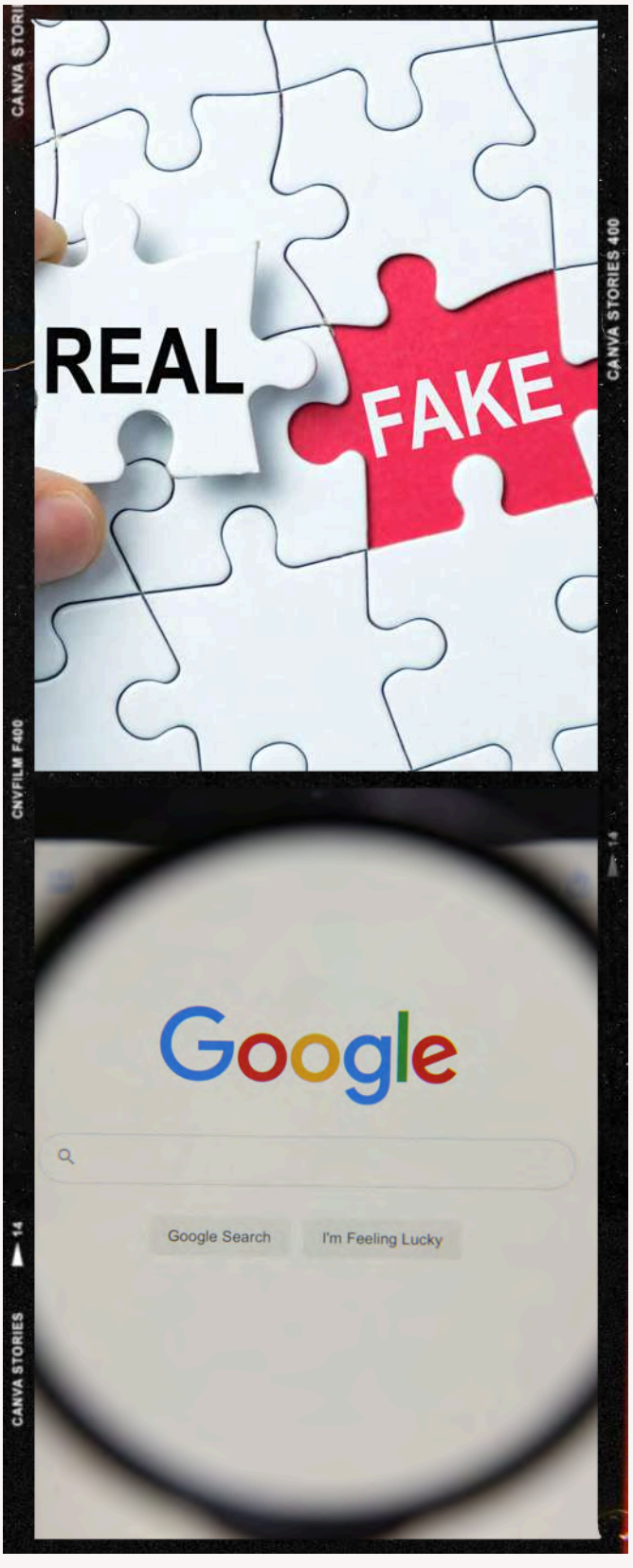
It's known as URL hijacking, sting sites, and fake URLs. Also commonly referred to as typosquatting, this practice is when cybercriminals take common spelling errors of a legitimate website to entrap would-be users into giving out private info. For example…

They might send you to g00gle.com instead of the real search engine; of course, real typosquatters tend to be a little more clever and unnoticeable..

Typosquatting might use something like...

- A common misspelling
- A likely misspelling
- Pluralizing a singular or vice versa
- Changing the top-level domain (.gov instead of .org)
- A foreign spelling or name for the domain (U.K. grey versus American gray)
- Using different alphabets with letters that look extremely similar to ours (the Greek alphabet's α, β, γ, δ, ε, ζ, η etc.)

Cybercriminals will even set up the site to look very similar to the original to further dupe visitors, like using the same color scheme or even stealing their images and logo. Beware of where you're inputting personal information, double-check URLs, and make sure the sites you're visiting are secure!



✓ Be careful when typing website addresses. Double-check the address before you hit enter.

✓ Use a password manager to create and store strong passwords for all of your online accounts.

✓ Be wary of emails or pop-ups that ask for your personal information. Legitimate websites will never ask for this information over email or pop-up.

✓ Keep your operating system and software up to date. This will help to protect you from malware attacks.

Protect yourself, and your systems, from typosquatting and all its consequences!

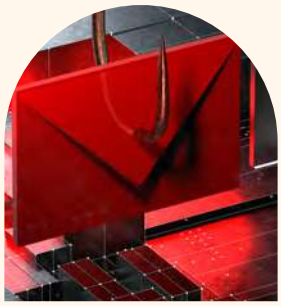
THE MORE YOU KNOW

560,000 new malware are discovered every day according to the AV-Test Institute.

4.1M websites are malware-ridden according to SiteLock Website Security Report 2022.

94% of malware comes via email, the Verizon DBIR found, hence why phishing remains such a big threat.

5.5B malware attacks occur yearly, SonicWall's 2023 Cyber Threat Report found. How many of them succeed?!?!



$7.2M and 560K records are impacted in an average ransomware attack, Comparitech found.

Nearly 500M ransomware attacks occurred in 2022, SonicWall found.

SPEED AWAY FROM FAST RANSOMWARE

Ransomware steals and encrypts files, and refuses to give you the decryption key until you pay a steep fee. Often, the bad actor refuses to return data regardless of whether you pay; and sometimes they even charge a second “double extortion” fee to prevent them from publishing all the stolen data online.

Sounds scary, right?

Well now, ransomware is even more frightening. “Fast ransomware” acts much quicker than the typical malware does, often working within minutes or even seconds of being deployed. This makes it difficult for victims to stop the encryption process before their files are locked up for good!

Typically in a ransomware attack, you would want to disconnect the infected machine and start incident response plans immediately. Time is always of the essence, but even more so when software can move this quickly!

Some of the fastest ransomware strains can encrypt files at speeds of over 100 GB per minute. This means that even large networks can be encrypted in a matter of minutes. Popular fast ransomware strains include...

- LockBit
- BlackCat
- MalasLocker
- 8BASE
- Akira
- Rorschach

Just like other malicious cyber software, fast ransomware is typically delivered through traditional cybercriminal methods, such as phishing and social engineering.

If you think you may have been infected with ransomware, remember: DO NOT PAY THE RANSOM.

Report the infection to your IT team and authorities. Hopefully, you have tried and tested backups that can recover your lost files for occasions like this!

How cam YOU protect yourself from fast ransomware?

- **Be careful about what emails you open and what attachments you download.**
- **Keep your software up to date, including your operating system, antivirus software, and web browser.**
- **Back up your files regularly.**
- **Have a plan in place for how to respond to a ransomware attack.**

"FAST RANSOMWARE ACTS MUCH QUICKER THAN THE TYPICAL MALWARE … WORKING WITHIN MINUTES OR EVEN SECONDS OF BEING DEPLOYED."

MALWARE GETS PHYSICAL

malware goes beyond digital infiltration...it can even infect and upset physical systems!

Here's something surprising that you may not have known about malware:

It can be used to control physical objects.

In recent years, there have been a number of cases of malware being used to control physical objects, such as cars, medical devices, and industrial systems. This type of malware is known as IoT malware, and it is becoming increasingly sophisticated.

The *Internet of Things* consists of less-secured devices that connect to WiFi, which tend to be less secure than your work computers that are backed by high-tech firewalls and overseen by security experts.

The ability of malware to control physical objects poses a serious threat to public safety and even national security!

This problem isn't new. As far back as 2010, a worm called Stuxnet was used to sabotage Iranian nuclear centrifuges. Stuxnet was able to control the centrifuges' speed, causing them to spin erratically and eventually self-destruct.

The threat to public safety has only grown in the decade-plus since. A vulnerability known as BlackBerry QNX let attackers remotely take control of a car's infotainment system and use it to launch attacks on other systems in the car. The vulnerability affected a wide range of car models, including Audi, Volkswagen, BMW and Mercedes-Benz.

Data privacy is a serious business, and organizations of all sizes have been experiencing an unprecedented number of attacks since so much of the world moved online. Stay up to date on the latest threats to your systems, and make good decisions about your online security every single day!

If you are concerned about the security of your IoT devices, you can also consider using a dedicated IoT security solution.

These include device discovery and identification, which discern all of the IoT devices on a network, even if the devices are hidden or behind a firewall. You can also scan these connected systems for vulnerabilities, such as missing patches that could be better secured with a software update.

A full security solution should also encrypt your data in transit and storage; as well as monitor traffic for malicious activity, so as to block unauthorized access and stop attacks before they do damage.

Can your IoT devices effectively detect, respond to, and recovery from security incidents?

Some other ways that you can help prevent attacks on your Internet of Things devices, include but are not limited to:

- **Keep your software up to date;** including the operating system, antivirus software, and firmware for your IoT devices.
- **Use strong passwords and enable two-factor authentication** for all of your devices, including IoT.
- **Only connect your IoT devices to secure networks,** because you never know who is lurking on public WiFi and spying on your connection!
- **Be careful about what apps and websites you allow access** to your IoT devices, because compromised sites can secretly download malware to your devices.

IoT devices can be valuable, but they can also pose security risks. By deploying an IoT security solution, businesses can protect their IoT devices, data, and networks from cyberattacks.

The human factor is the weakest link in the security chain.

-Marcus Ranum

The MacGuys+
Work From Anywhere
Mac IT Support

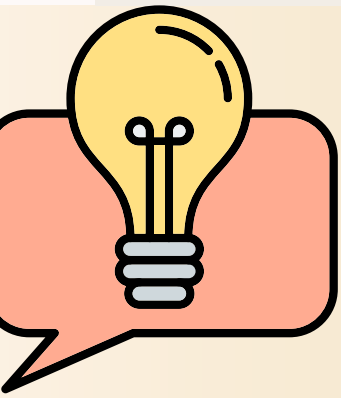
https://www.themacguys.com/123
linkedin.com/company/themacguys/

facebook.com/themacguys
twitter.com/The_Mac_Guys
youtube.com/c/TheMacGuys

Connect with our featured guest!

Looking to take your security to the next level? Do you want to keep up to date with the best ways to stay cyber-safe, the new gadgets and features that combine convenience and efficiency, and breaking news in the tech industry?

 Cyber Sight Publications



TECH TIP FROM THE MACGUYS+

A weak password is still one of the most common ways hackers break in!

Thanks to sophisticated brute-force-attack software readily available online, hackers can try ***tens of millions of possible password combinations per second.*** *For example, hacking software can guess a five-character password in under three hours.* ***If you only use lowercase letters, it's 11.9 seconds!***

If I was to change one thing to help improve everyone's security, it would be to use better passwords and MFA whenever possible!