FEBRUARY 2023

ISSUE NO. 41

THE DIGITAL DOWNLOAD

Cyber Sight Publications

TIM NYBERG, CEO OF THE MACGUYS+

on What to Do If Your Data Is Exposed

Page 12

HOW TO PROTECT YOURSELF FROM MALWARE

Page 19

REAL WORLD CYBER-ATTACKS IN 2022

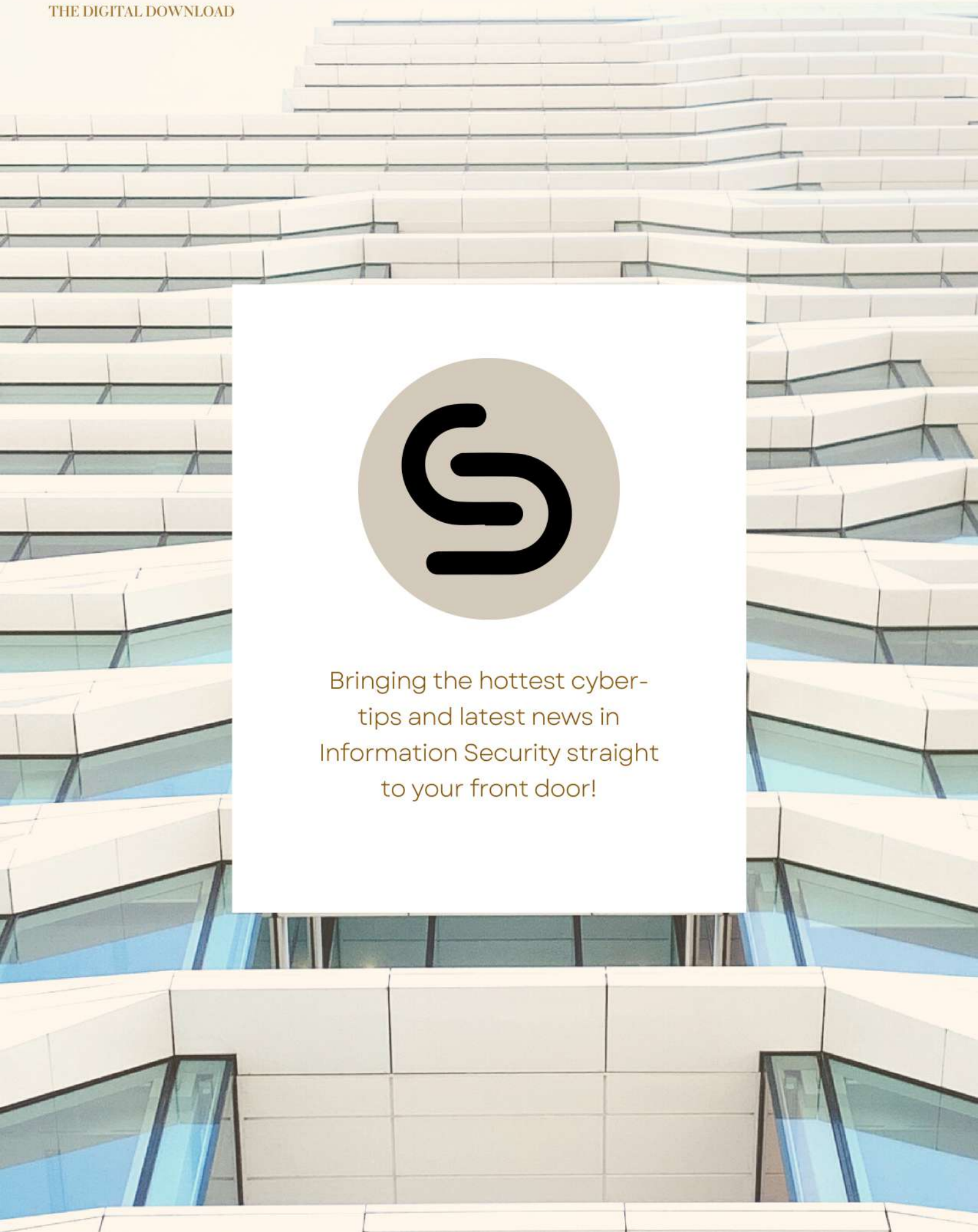
Page 16

ANSWERS TO YOUR TOP TECH FAQs

Page 6

360°

coverage, all year round



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

TABLE OF CONTENTS

360°

coverage, all year round

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!

ANY SUFFICIENTLY ADVANCED TECHNOLOGY IS INDISTINGUISHABLE FROM MAGIC

-Arrthur C. Clarke

TOP 5 TECH FAQS

Answers to the tough questions YOU have about cybersecurity

When technology doesn't work the way it's supposed to, it can get frustrating pretty quickly. The running joke in I.T. is that tech experts spend all day in a cubicle, telling customers to "try turning it off and then on again." While that might work some of the time, often the problem goes deeper than that.

Now, you may be thinking: *How often do I really have computer problems?* Even someone who primarily logs online to check their email and buy some furniture will eventually find their mouse lagging, browser freezing or battery shutting down too quickly.

Know what you're up against before it's an emergency! Your "first aid kit" has arrived so you never have to go through the rigamarole of tech support again.

#1 My WiFi is so slow, please help!

Is it taking five minutes to load a single page? The first step to testing what's wrong with your Internet is to check the speed on different devices. If your laptop is having problems connecting to the web, try it on your phone. If the phone launches every site just fine, you can narrow down the issue to the computer; or if WiFi lags on the phone too, it's likely a problem with the router.

If it's the device: Close out of all your tabs except the one you want to use. Cluttered browsers need more CPU to run, which is why you might hear your computer's fan working overtime when you launch the Internet. Closing tabs limits the power it has to exert to open the web browser. Alternatively, you might have too many walls or too much space between the device and WiFi router. Move them closer together to improve the connection.

If it's the router: You may need to buy hardware that expands the range your WiFi can reach. If the only place to put the router is the basement, it will have trouble reaching through three concrete floors without assistance. If proximity isn't the problem, call your Internet provider to find out about potential outages in the area or to get a technician out to look at it in person.

#2 My computer keeps shutting down, what's happening?

There are several reasons this could be happening. If your device feels very hot to the touch, likely it overheated from a software that it couldn't handle or spent too much time in the sun. If it's not warm to the touch, it could simply be an old hard drive or battery that doesn't work so well anymore. The only fix there is to replace the malfunctioning part.

Perhaps the device won't turn on at all. No lights or sounds is likely an issue with the power. If possible, take out the battery. Then plug it into a reliable outlet and see if that lets you boot it up. From there, you can assess if it has trouble holding charge or has self-diagnosed a problem at startup.

When all this fails, take the device to a technician who can diagnose the issue and replace the faulty parts.

#3 What is the Cloud and is it safe?

The Cloud is an external storage system that automatically saves and stores data. There are many different kinds of Cloud services; it simply refers to an external server, as opposed to a physical system that you connect to your devices to back them up on a regular basis. Choosing Cloud storage protects your backup files from physical damage, theft or loss. They usually save your files automatically so you don't have to remember to do it at the end of the week or month.

Meanwhile, people worry about the ability to hack into Cloud servers since they operate remotely. That's why smart password protection is a must. This will secure your data while simultaneously giving you easy access to backup files and let you access that information from any internet-enabled device.

If you do shop online, consider securely storing this information by using a Password Manager like 1Password.

#4 Is it bad to use free public WiFi?

When you're out on the town, the first thing you do when you settle down at a table is look up the establishment's WiFi and pray there's something free nearby so you don't run up your 4G or 5G.

The problem is, public networks are an easy way for threat actors to hack into insecure devices. Even if they have a password, like Guest WiFis often do, others with the password can potentially see what you're doing and even steal credentials if you log into apps like your bank account. Circumvent some of these risks by making sure all URLs you visit are HTTPS (the "S" stands for secure) and use a VPN unless you trust the network you're using.


11.11
FORMATIONS
GALERIE TEMP

#5 How can I identify spam and scams?

Some spam is obvious, with misspelled product labels and faulty grammar all throughout the message. Some, however, are harder to identify: They address you by name, have a reputable company header on the landing page and the URL looks legitimate. How can you tell them apart from real, secure websites?

- It's surprisingly easy to disguise a hyperlink as some other text. Right-click on links to copy and paste them into a separate tab yourself, to verify the URL matches what the link purported
- Check for contact information on the landing page. Legitimate websites should have an easy way for you to contact customer service
- Don't click attachments you're not expecting. These are common vessels for malware; real websites will direct you how to complete tasks on their secured website instead of expecting you to blindly download files
- Make sure the websites you visit start with HTTPS instead of HTTP. The "S" stands for secure and certifies that communication is encrypted

When in doubt, slow down and follow your intuition. Caution is always preferable to recklessness when phishing scams are at risk.

CHECKLIST

to keep your computer running smoothly

- ☑ *Don't rush into big OS updates*
- ☑ *Shut down PROPERLY each night*
- ☑ *Clear the Trash and Downloads*
- ☑ *Remove old, unused programs*
- ☑ *Regular maintenance*

TECH TAKES US TO NEW HEIGHTS...

"When digital transformation is done correctly, it's like a caterpillar turning into a butterfly."

-George Westerman, Principal Research Scientist at the MIT Sloan Initiative on Digital Economy

WHAT TO DO IF YOUR DATA IS EXPOSED

with Tim Nyberg, Founder & CEO of The MacGuys+

Things are always changing with every update for our devices. It is important to check the privacy and security settings, as well as location services settings, after every update. This will help ensure you are leveraging every possible security option that you can, to best protect your data and privacy.

Unfortunately, security incidents aren't uncommon despite our best efforts to maintain cyber hygiene. If data gets leaked, then transparency is the best policy. Attempting to cover up the event will end up costing you more than the breach, so it's best to always come clean.

FEATURING TIM NYBERG

CEO OF THE MACGUYS+

WHEN THE WORST HAPPENS

No matter how careful you are, the event of your data being caught up in a breach is a matter of WHEN...not IF. Should you become aware that your own personally identifiable information (PII), and others' data that is under your management has become compromised, there are steps you can take immediately to reduce the harm inflicted.

The first step is to be calm, contact your IT team and check your data breach protocols. Some of those actions may be such things as updating all your passwords, starting with the most critical sites first and following all the standard rules for passwords.

Contact any companies that might have been affected by that breach, and put those accounts on hold while you assess the extent of the breach.

If the breach affected client data, then you should contact those clients and let them know the situation, so they can take any steps they might personally prefer to take as well.

If you have a data breach plan in place, you could send out a document filled with guidance for your clients on how to handle the situation.

If there is a significant loss of funds, generally tens of thousands of dollars or more, you can also contact the FBI's cybersecurity division, but they are not likely going to be interested in small cases because they handle so many. If you get the authorities involved, you should call as soon as possible to increase the chances of any kind of successful outcome.

Having a well-thought-out plan ahead of time is very important. Some other things of consideration are backups, network security, employee training, etc.

If I was to change one thing to help improve everyone's security it would be to use better passwords and MFA whenever possible. Here is a set of solid guidelines to help make that a little easier:

You KNOW you need to have a better password than “password” or “letmein” if you have any hope of keeping hackers out of your computer, but what does a “strong” password mean?

A good password should be **at least twelve characters long** (or longer!) and have a **combination of uppercase and lowercase letters, numbers, and symbols** that are hard to guess. Don’t use dictionary words with proper capitalization because they’re easy to guess (like Password1234#). Even though it meets the requirements we just discussed, it’s easily hacked; remember, hackers have sophisticated password-hacking software that will run 24/7/365.

This is an example of a few bad passwords:

- password
- 12345678
- Kitty1234!
- JimBob222!

This is an example of a good password:

- r_aQGvH99io6CCJz

As you can see, you will never remember a good password, or if you can remember a few, you won't remember all of them. Use a password manager such as 1Password to manage your passwords and use it to generate passwords for you. **If you can remember the password, it isn't a good password.** If you are on a Mac, you can use Keychain and accept the suggested passwords, or even manage them in the built-in password manager.

It matters not what kind of computer you use; Mac or PC, passwords are one of the weakest links in your security!

Visit our website to know more!

themacguys.com

Real Life Threat Example:

RACCOON STEALER MALWARE

First making headlines in 2019, the Raccoon Stealer malware originated on the Dark Web and quickly proliferated. This isn't just because the sole perpetrator got busy, but because they're able to sell subscriptions to buyers on the Dark Marketplace. Thanks to what's known as malware-as-a-service, threat actors quickly overtook hundreds of thousands of devices.

Operations briefly ceased following the Russian invasion of Ukraine, or so the developers claimed. Reportedly one of their group members had been killed in the conflict and they ceased operations for several months. Raccoon Stealer went quiet.

Just three years after its initial discovery, Zscaler analysts indicate that a new version of the Raccoon Stealer malware is back in 2022 with greater challenges for the machines it infects.

This particular infection goes by several monikers. Also known as Legion, Mohazo and Racealer, it is actually a trojan which disguises itself as a benign file or program to convince you to download or click on the link. After it's on your device, the hidden malware executes.

Cybercriminals who use Raccoon Stealer can purchase logs of stolen information directly. Instead of launching the attack, they simply buy, for example, a bundle consisting of your Facebook login information. Then the purchaser can log on, blast phishing messages to all of your friends and even steal money or crypto funds.

Trojans rely on appearing like legitimate software, so you have to slow down and really assess new files before downloading them. In 2022, Trojans made up more than half of malware infections around the world.

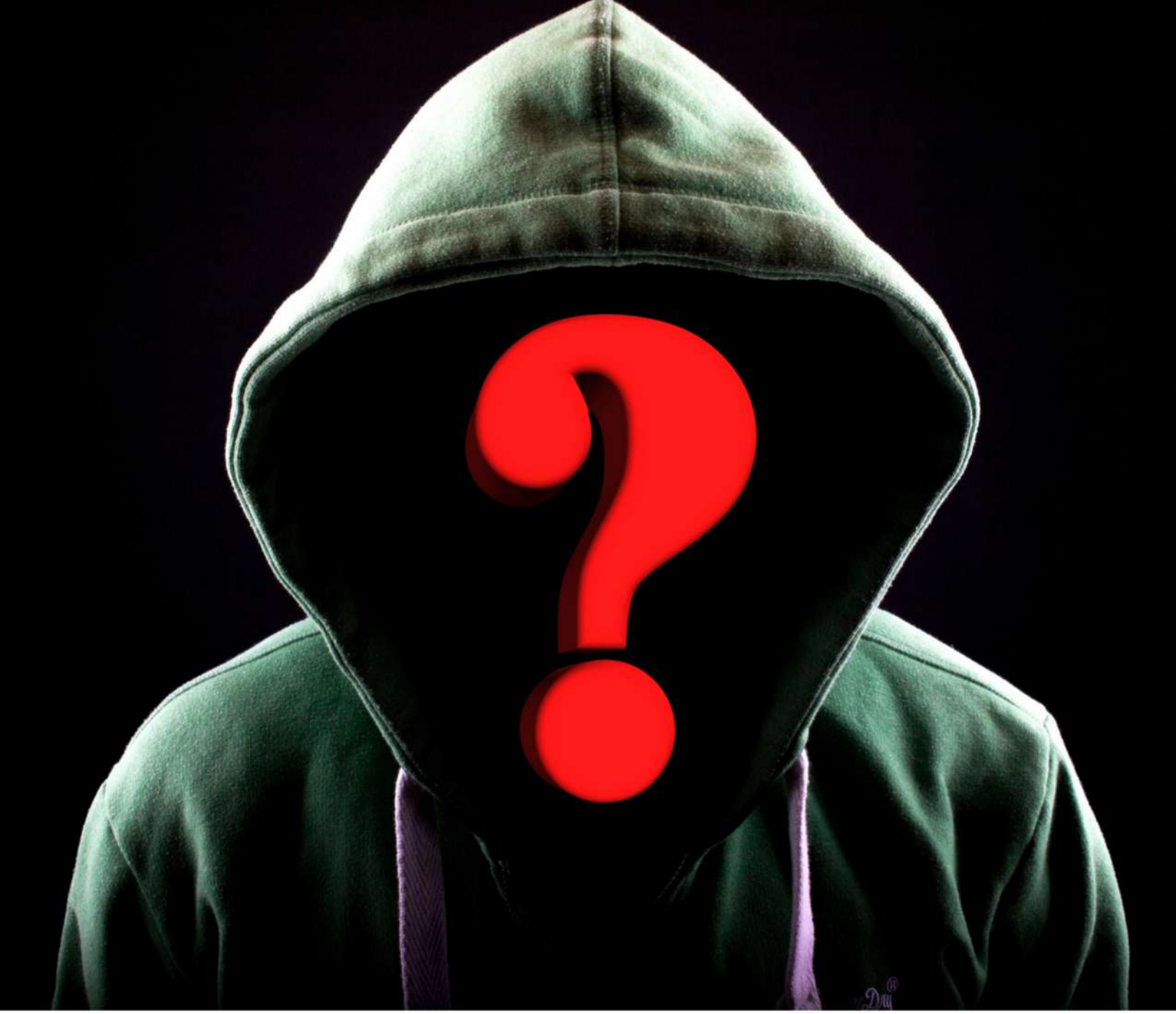
"THE NEW VERSION THAT HAS BEEN INFECTING MACHINES IN 2022 IS MUCH MORE EFFECTIVE "

Raccoon Stealer malware infects targeted machines to steal credentials from their users. The malware is capable of all kinds of malicious acts, such as...

- Targeting particular apps
- Recording fingerprint information
- Stealing passwords and log-in information, especially autofill data
- Stealing saved cards and cryptocurrency
- Viewing cookies, programs and more
- Access your downloaded programs, as well as all of their data
- Using hacked accounts for purchases

The new version that has been infecting machines in 2022 is much more effective at completing these awful goals. The new malware is written in a different programming language (C as opposed to C++) which is slightly smaller and therefore works faster, though lacking various features. However, this also happens to make it more efficient at committing theft than the first Raccoon Stealer malware.

The newer version is also capable of running on both 32- and 64-bit systems without dependencies. In summary, it's a dangerous variant that is projected to grow more capable and remain a household name.



"UPGRADES…WILL HAVE BETTER SECURITY FEATURES AND PROTECTION FROM ZERO-DAY ATTACKS."

PROTECTING YOURSELF FROM MALWARE

Regularly update your antivirus software to best protect yourself against the Raccoon Stealer trojan, as well as any other malware you might come up against in the future. Automated system scanners alert you instantly to suspicious activity, while Dark Web monitoring can tell you as soon as your PII (personal identifiable information) appears on the dark marketplace for cybercriminals like Raccoon Stealer subscribers to purchase. Mac or PC you need to properly protect your systems.

ZERO-DAY ATTACKS: A zero-day attack is when hackers take advantage of a vulnerability developers don't know about. Developers are completely unaware of the weak point until after the attack occurs.

Continuous monitoring matters! Automated scanners can regularly check the health and safety of your system without your manual intervention.

Make **software and system upgrades** ASAP! The latest versions will have better security features and protection from zero-day attacks.

Despite any hardware or software precautions you may be taking, you still need to **BOLO** (be on the lookout) for any suspicious activity!

"Communication – the human connection – is the key to personal and career success."

– Paul J. Meyer

REAL LIFE THREAT EXAMPLE:

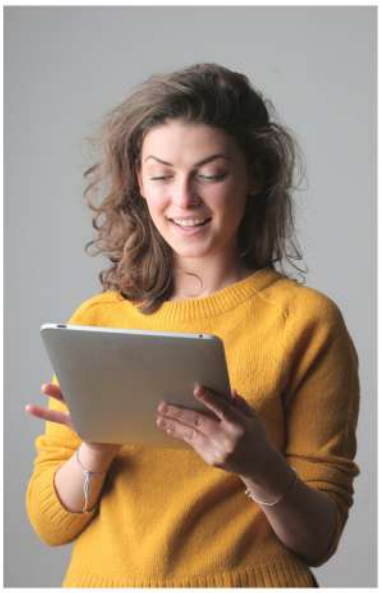
LASTPASS BREACH 2022

WHAT'S LASTPASS?

Password managers are a great way to keep secure, varied credentials on all of your different accounts. They let you log in and out of your favorite sites without having to worry about forgetting all those confusing strings of letters, numbers and different capitalization.

What happens when a hacker breaches that massive log of data? That nightmare came true for LastPass users in late August 2022.

THE BREAK-IN



In the unfortunate case of LastPass, a developer's account was actually compromised first. Although it's never fun to have your accounts hacked, choosing a developer for a target gave the hacker immediate access behind-the-scenes.

The hacker targeted the development side of the app, stealing source code and other propriety information. They say that no user information has been compromised, including Master Passwords that would put their credentials and entire information vault at risk.

ABOUT YOUR DATA

Their Zero-Knowledge security model means that even LastPass developers and higher-ups don't have access to your Master Password, thus this breach wouldn't put that information in harm's way.

LastPass responded to the breach, writing on their blog, *"In response to the incident, we have deployed containment and mitigation measures, and engaged a leading cybersecurity and forensics firm. While our investigation is ongoing, we have achieved a state of containment, implemented additional enhanced security measures, and see no further evidence of unauthorized activity."*

Is All of My LastPass Data Safe?

The good news is that there was no evidence of malware or some exploitation of the software which could harm your encrypted password vault. Most sources, both inside and apart from LastPass, suggests that there's no real need to change your passwords, but if you're feeling uneasy, you can change your Master Password (you should do this anyway, just like it's recommended to change any other password every three months or so if you don't have two-factor authentication and a complex, unique password).

You might also consider switching to a password manager with open source coding, as it will have more transparency in how it works and thus more eyes out for potential vulnerabilities.

WAIT!

SAFE PASSWORD CHECKPOINT!

Does your password...

- ☑ *Use letters, numbers, & symbols?*
- ☑ *Change every 3 months?*
- ☑ *Stay unique for each account or site?*
- ☑ *Avoid references to your PII?*
- ☑ *Stay private so ONLY you know it?*

The MacGuys+
Work From Anywhere Mac IT

themacguys.com

Proudly servicing the Minneapolis-St. Paul Metro area and Western Wisconsin

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?

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!