JANUARY 2023 ISSUE NO. 41

THE DIGITAL DOWNLOAD

Cyber Sight Publications

KONRAD & KEVIN MARTIN, FOUNDERS OF TECHADVISORS, INC.

are the "Twin Tandem Tough on Cybercrime"

Page 12

ANSWERS TO YOUR TOP TECH FAQs

Page 6

REAL WORLD CYBER-ATTACKS IN 2022

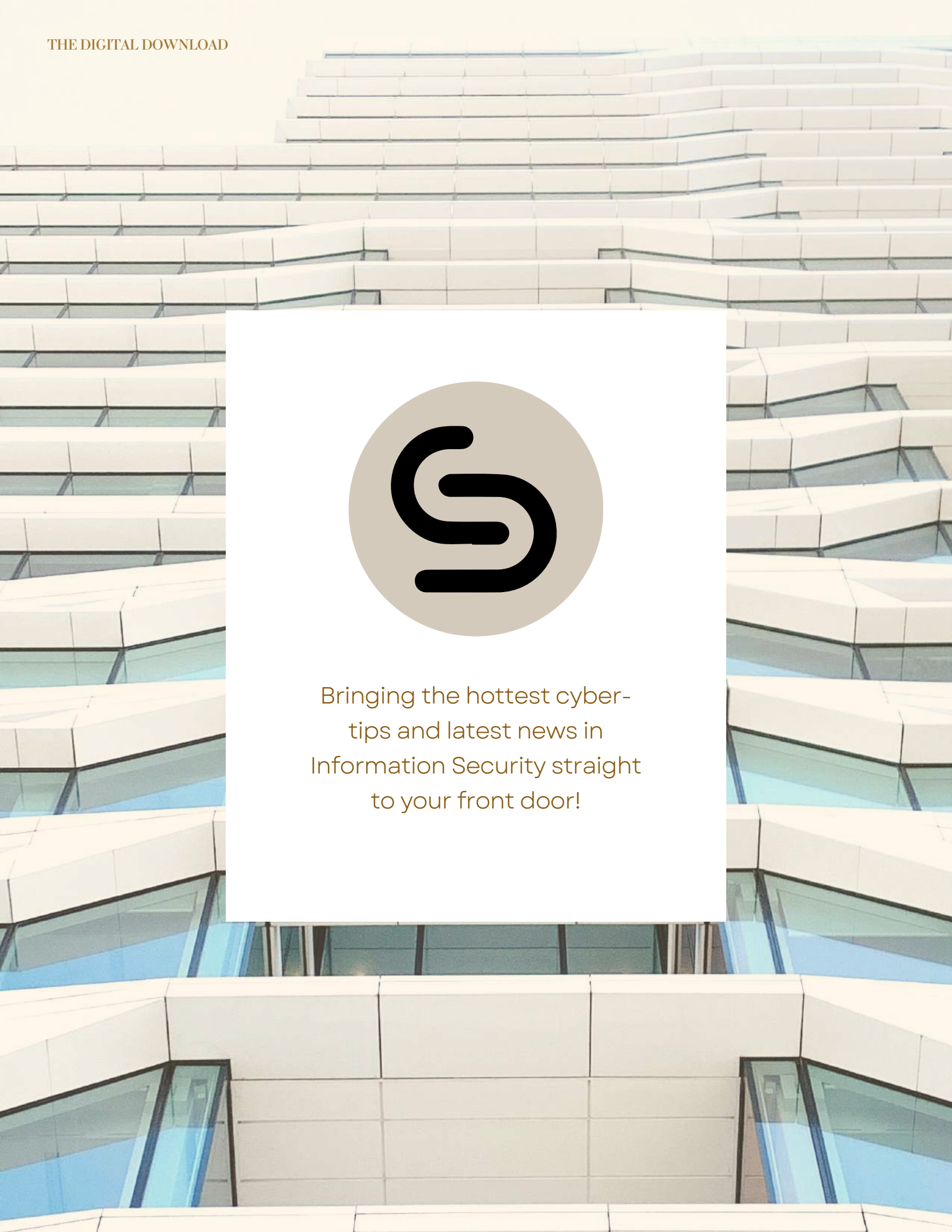
Page 16

HOW TO PROTECT YOURSELF FROM MALWARE

Page 19

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

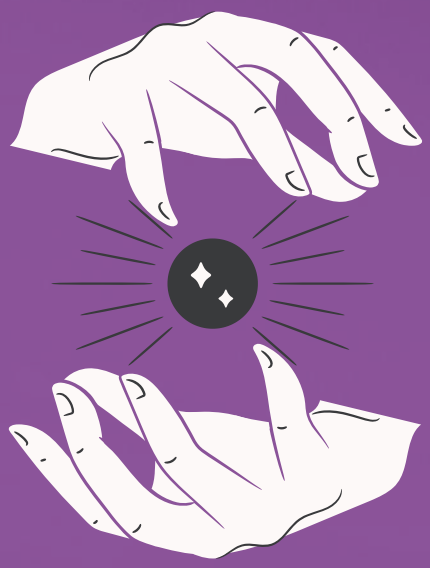
EDITOR'S NOTE

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 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.

#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 TEMPO

#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

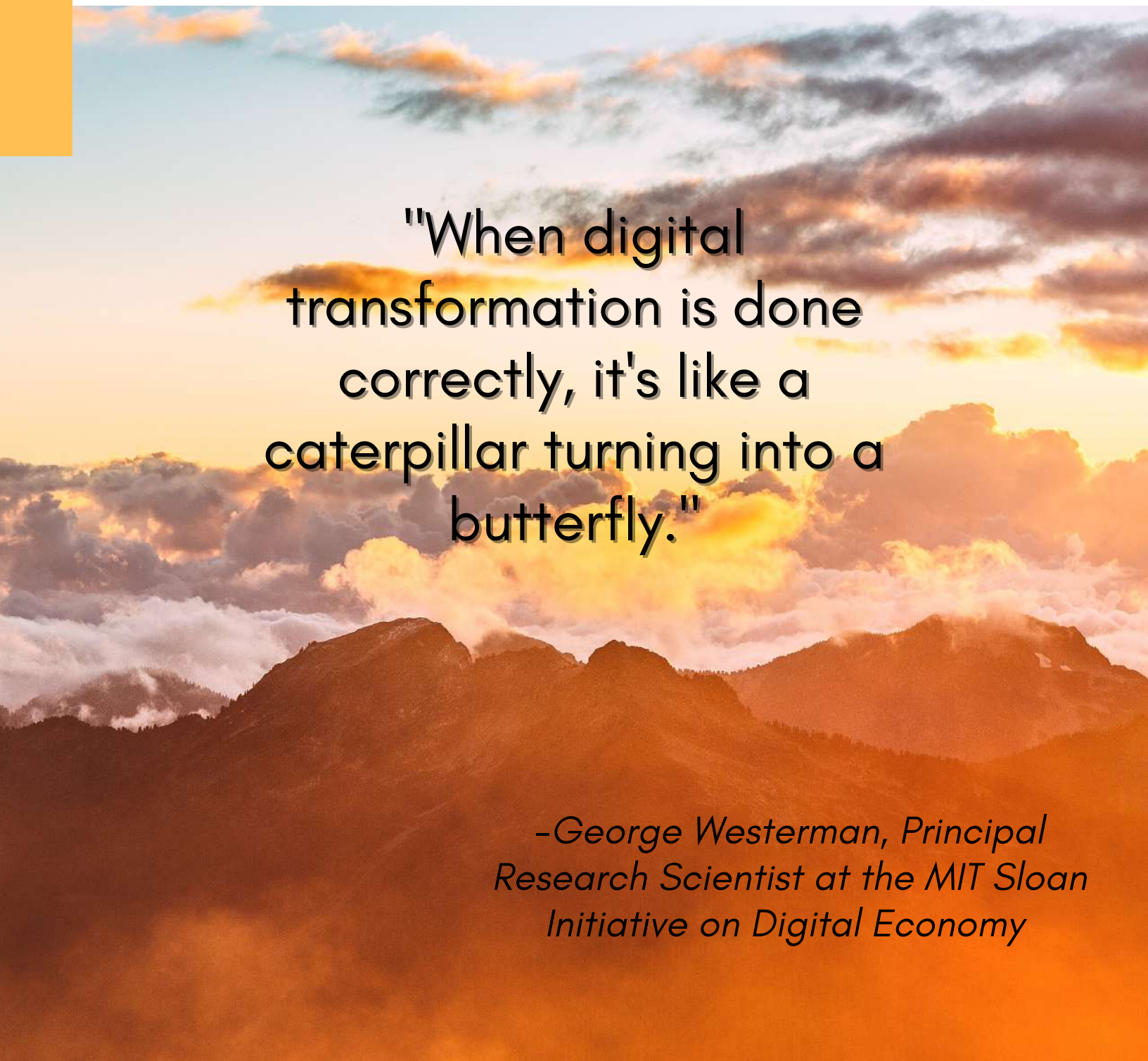
When in doubt, slow down and follow your intuition. Caution is always preferable to recklessness when phishing scams are at risk.

CHECKLIST

to keep your computer running smoothly

- ☑ *Set updates to run automatically*
- ☑ *Shut down PROPERLY each night*
- ☑ *Clear the Recycling Bin*
- ☑ *Remove old, unused programs*
- ☑ *Clear browser cookies and history*

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

TWIN TANDEM TOUGH ON CYBERCRIME

with KONRAD & KEVIN MARTIN

As twins, we've always done a lot of things together. We both competed in the pool together (Kevin was an All-American diver; Konrad swam competitively in college), we both graduated from the University of Maine together, and we both initially became CPAs early in our careers. And eventually, we both took the risk of leaving our salaried positions at a reputable accounting firm to launch our own business, which aimed to meet the technology needs of other CPA firms.

This decision stemmed from recognition of a real need among our colleagues – to provide high-level technical support quickly and effectively.

The fact that we were former CPAs helping other accounting firms added great value to what we offered – we understood how they required the technology to work, and could fulfill those requirements fast. But soon we learned that what we offered accountants could easily be applied to other small and mid-sized businesses too. While our client base was initially comprised almost exclusively of CPA firms, now about half of our business comes from other professional services sectors.

"Everyone needs to take cybersecurity seriously."

KONRAD & KEVIN MARTIN

OWNERS OF TECH ADVISORS

When we started Tech Advisors more than 15 years ago, cybersecurity was barely in our lexicon. Quickly, though, with the ever-changing landscape, we understood how crucial cybersecurity is to our clients, and we've grown to become the preeminent managed security provider on the East Coast. Kevin (always the real techie) keeps us on the cutting edge with regard to technology – constantly determining and reconfiguring various security stacks to help us stay ahead of hackers worldwide. He's especially keen on the MDR-SOC and SIEMs – they are invaluable tools in the cybersecurity fight. Konrad is great at communicating the importance of cybersecurity, and has contributed many articles, books, and even a film, which is expected to premiere early in 2023.

One thing we've definitely noticed over our years in cybersecurity, and especially recently, is the increasing frequency of phishing attacks. Certainly the commonality of these attacks makes it more likely for people to fall for them, but hackers are also becoming more sophisticated all the time. Spear phishing is the latest incarnation, weaving in personal data about someone to make the request all the more plausible. What's most important about this is it must be taken seriously, and one of the biggest mistakes someone can make about phishing is, "I'm too smart to fall for a fake email." It doesn't matter what position you hold in a company, what level of college you finished, or how much you make – we've seen everyone click on something they shouldn't have.

As the number and severity of ransomware threats continue to increase, the best way to combat this is to increase and enhance overall cybersecurity training. This is vital to not falling victim to ransomware. Most people don't stay cognizant of the fact that they are not alone online. Training goes a long way toward helping to build that self-awareness and break any bad habits users have developed.

Personal devices are another easy way for hackers to get into a network. We've developed and encourage MDM – Mobile Device Management. This policy makes sure devices used are connected to a protected, secure server, and includes best practices for what people should – and should not – use their mobile devices for.

Also, unfortunately almost everyone has data on the Dark Web – but if it's remediated quickly, it's certainly not the end of the world. When we uncover it, the quickest and most effective solution is for the affected person to change their password associated with the information, and to never use that password again!

We use both remote and physical servers. We encourage our clients to move to the cloud, as the benefits are numerous (with safety at the top of the list), but we understand it's still a hard sell for some people, and so are happy to meet them where they are while still keeping them cybersafe. Backups should be tested once a month at minimum – every other week is optimal.

The recent Optus data breach in Australia points to the importance of cybersecurity standards, typically outlined through various compliance measures. While no one likes compliance, we'd hasten to bet that breaches are WAY less popular. Plus, most cybersecurity compliance regulations are common sense, and meant to protect your business *and* your clients.

Should a breach occur, credit monitoring and changing of passwords are the two biggest things you can do. Stay alert and watch for any suspicious activity – the quicker you see it, the quicker you can stop it. And if you're in the unenvious position of having your clients' data exposed, your best bet is quick and personal outreach – a phone call is best, especially if the number affected is low. That conversation should include tips on what they should do to mitigate any negative fallout, and how you'll help with that.

All of our years of experience, access to the best and most cutting-edge technology, and
intensive and consistent training has taught us one thing – everyone needs to take cybersecurity seriously. Repetitive, consistent training with reminders to stay vigilant, and humility to remember that you don't know what you don't know. The internet is like a public highway that's digital.It's up to all of us to be cautious, aware, and responsible while on this digital public highway.

Back when we were swimming together, we gained a reputation as a "twin tandem tough to beat." When it comes to hackers, we're proud to say that still holds true.

TECH ADVISORS

IT Support and Cloud Management

"The way to combat [more ransomware] this is to increase and enhance overall cybersecurity training."

Visit their website to know more!

https://www.tech-adv.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.

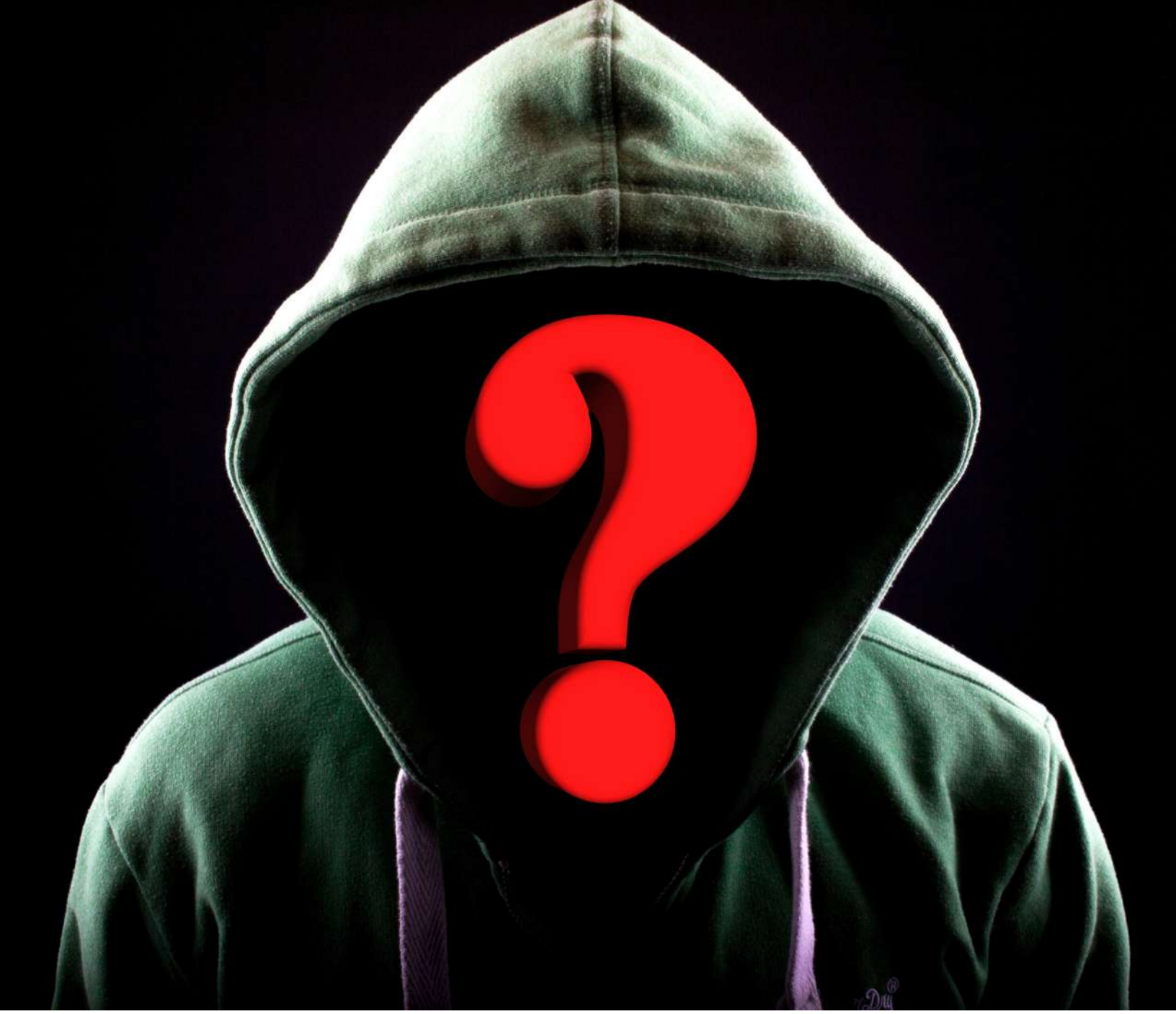
"THE NEW VERSION THAT HAS BEEN INFECTING MACHINES IN 2022 IS MUCH MORE EFFECTIVE "

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.

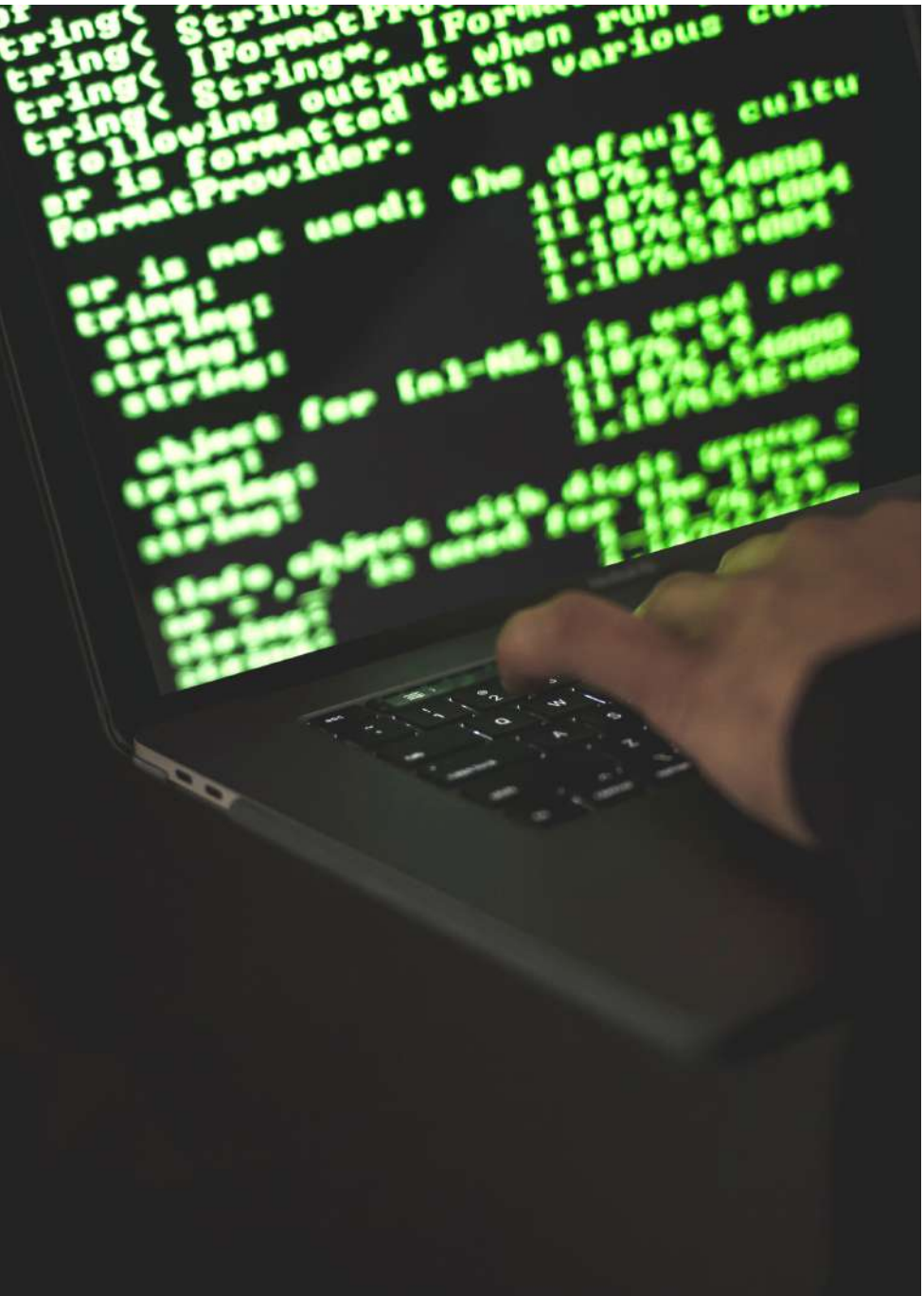
The newer version is also capable of running on both 32- and 64-bit systems without dependencies. In summary, it's a dangerous variant that is projected to grow more capable and remain a household name.



"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.



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 soft- and hardware, you should always **BOLO** (be on the lookout) for unusual activity on your networks and accounts!

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

– Paul J. Meyer

REAL LIFE THREAT EXAMPLE:

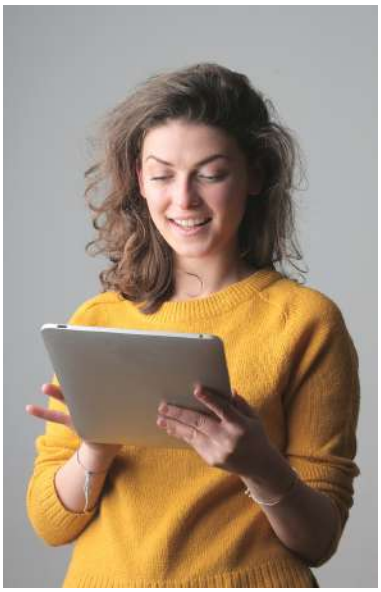
LASTPASS BREACH 2022

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?*
- ☑ *differ between accounts?*
- ☑ *avoid references to your PII?*
- ☑ *stay private so ONLY you know it?*

TECH ADVISORS

ticketing@tech-adv.com123
75 State Street, Ste 100, Boston, MA 02109

www.tech-adv.com
https://www.facebook.com/techadvinc
https://www.linkedin.com/company/tech-advisors-inc

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?