pcplus networks
better people, better solutions
1010 Lakes Pkwy
Lawrenceville, GA 30043

TRIVIA

What does the ZIP in ZIP file mean?

A. Zigzag Insertion Point
B. Zonal Integrated Process
C. Zero Information Packaging
D. Zipped Information Protocol

Answer: A. ZIP in ZIP file stands for "Zigzag Insertion Point" because it compresses data like a zigzag.

BEWARE OF WIFI SQUATTING

When did you last check who has access to your WiFi network? If it's been a while, you'll probably be surprised by who's hanging around. Managing your WiFi access is an important step to keeping your data safe because unwanted WiFi squatters could, at best, slow your WiFi speeds and, at worst, have access to any device or file connected to your network, like household security cameras. To see who has access to your WiFi, find your router's IP address (you can find instructions online about how to do this), type the IP address into your browser and log in. Next, look for a list called "DHCP Client" or "Connected Devices." Review the list, and if any unknown devices are on it, update your WiFi password and reconnect only the devices you trust.

ARE YOU MANAGING YOUR VENDOR SECURITY RISKS?

As the year winds down, innovative businesses often reflect on what's gone right – and what needs improvement. Beyond wrapping up projects and planning for next year, one critical task shouldn't be overlooked: managing vendor security risks. Vendors play an essential role in your business's success, but they also present a severe cybersecurity risk if you don't vet and monitor them effectively, especially if they handle sensitive data.

What's A Vendor Risk?

Many businesses rely on trusted vendors, such as cloud services or file-sharing tools, to carry out day-to-day operations. If that vendor gets hacked, your sensitive data is suddenly – and dangerously – exposed. A perfect example is the 2023 MOVEit Transfer breach, where attackers exploited vulnerabilities in the vendor's software, giving them access to critical data like customer information and business records for thousands of organizations. BlueVoyant's State of Supply Chain Defense report showed that organizations experienced, on average, 4.16 supply chain breaches in 2023 that impacted operations.

Vendor breaches are more than annoying – they could also lead to data loss, diminished customer loyalty or even legal issues. This year, consider adding these best practices to your end-of-year review to manage your vendor risk:

1. Review Vendor Contracts
Like you, vendors need to be held accountable for following industry-standard practices like encryption, secure data storage and incident response protocols. Start your vendor risk review by checking to see if your contracts have the necessary security clauses, and make sure your agreements outline these expectations clearly so you and your vendors know what's at stake.

2. Conduct Vendor Security Audits
If you haven't done it recently, it's time for a thorough security audit of your high-risk vendors. This will help you understand if they're implementing strong cybersecurity measures, such as multifactor authentication, encryption and regular system updates. Knowing where your vendors stand gives you a better handle on your own security.

3. Monitor For Emerging Risks
Cyberthreats evolve quickly and so do the risks your vendors face. Regular monitoring of your vendor's security practices, like tracking vulnerabilities or breaches, will keep you on top of any emerging threats.

4. Update Your Vendor List
Now is a good time to clean house. Cut ties with vendors who aren't living up to your security standards and tighten your relationship with those who are proactive about protecting your data. Consider creating standardized onboarding and offboarding processes for vendors, too, so old vendors don't have unwarranted access to your organization.

pcplus networks
better people, better solutions
Real World Tech Tips
Delivering Guaranteed Uptime, Speed, Security & Compliance

DID YOU KNOW?

Here's a common scam: you get an e-mail from the boss (or your spouse, parents or other trusted person) asking you to send them a copy of employee pay stubs, tax information or other files with confidential data such as social security numbers in them, or they're asking you to transfer or ACH payment to a vendor or a different bank account.

The problem: even though it is coming from an e-mail address of someone you know and trust and looks legit, there's a chance it could be a scam. Hackers can intercept e-mail messages and modify them.

If you ever get this kind of request, double-check by calling that person to confirm. And even if it turns out to be a legitimate request, you should never send confidential information like social security numbers (or attachments with this information inside them) without taking precautions to password-protect and encrypt the message first.

This monthly publication is provided courtesy of Shan Dholaria,

CTO of PcPlus Networks

OUR MISSION:

"As a business owner, you don't have time to waste on technical and operational issues, plus security is a BIG concern too. That's where we shine! We specialize in helping businesses streamline their IT, avoiding downtime by providing #1 Network Support, best-in-class Managed IT Services & Top-Notch Cyber Security solutions that deliver Guaranteed Uptime, Speed, Security & Compliance."

According to *TechCrunch*, this year has seen some of the most damaging data breaches in history. In 2024 alone, hackers stole billions of personal records, and it's almost guaranteed your data is among those stolen records. Let's look at this year's record-breaking attacks and what you need to know about protecting your information.

1 National Public Data
(2 Billion-Plus Records)

What happened: In December 2023, hackers accessed the systems of National Public Data, a background-check company. In April, 2.7 billion records with highly sensitive data for 170 million people were leaked onto the dark web.

Who is exposed: The stolen data includes records for people in the US, Canada and the UK.

Compromised data: 2 billion-plus records containing full names, current and past addresses, Social Security numbers, dates of birth and phone numbers.

2 Change Healthcare
(38 Million Records)

What happened: In February, the UnitedHealth-owned tech firm Change Healthcare was hacked by a Russian ransomware gang that gained access through systems unprotected by multifactor authentication. The attack caused widespread downtime for health care institutions across the US

continued on page 2...

...continued from cover

and compromised data for many, many Americans. UnitedHealth paid $22 million to prevent data leaks, but another hacker group claimed to still have some of the stolen Change Healthcare data.

Who is exposed: Estimated data exposure for one-third of the American population (likely more).

Compromised data: Payment information, Social Security numbers and medical data, including test results, diagnoses and images.

3 AT&T
(Hacked TWICE)

What happened: In March, hackers released data for more than 73 million past and existing AT&T customers going back to 2019. Then, in July, data was stolen from an AT&T account the company had with data giant Snowflake (more on that in a bit). Reportedly, AT&T paid a ransom to the hackers to delete the data. However, if this data is leaked, it could expose the data of anyone called by AT&T customers, including noncustomers.

Who is exposed: 110 million-plus past and current customers and, potentially, noncustomers.

Compromised data: Personal information, including Social Security numbers and phone numbers.

4 Synnovis
(300 Million Patient Interactions)

What happened: In June, a UK pathology lab, Synnovis, was attacked by a Russian ransomware gang. The attack resulted in widespread outages in health institutions across London. Reportedly, Synnovis refused to pay the $50 million ransom.

Who is exposed: Past and existing patients in the UK.

Compromised data: 300 million patient interactions, including blood test results for HIV and cancer, going back many years.

5 Snowflake
(600 Million-Plus Recordings And Growing)

What happened: In May, cloud data giant Snowflake announced a system breach caused by stolen employee credentials. Hundreds of millions of customer records were stolen from Snowflake customers, including 560 million from Ticketmaster, 79 million from Advance Auto Parts and 30 million from TEG.

Who is exposed: Millions of customers from many of Snowflake's 165 corporate customers, including those mentioned above, plus Neiman Marcus, Santander Bank, Los Angeles Unified School District and many more.

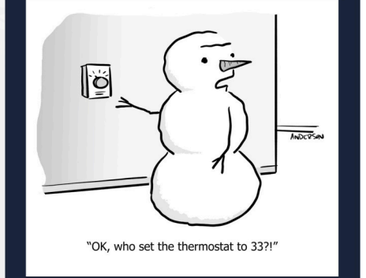
Compromised data: Customer records.

How To Protect Yourself

You can't stop companies from getting hacked. However, you can prevent the situation from worsening for YOU by taking a few extra steps to protect your data. Here's what to do:

- **Review your health-related communications:** With so many breaches affecting health institutions this year, pay attention to your statement of benefits and look for services you didn't receive. If you spot something fishy, tell your health care provider and insurance company right away.
- **Freeze your credit:** This will stop criminals from opening a credit card or loan in your name.
- **Update your log-in credentials:** If you know what accounts were hacked, change your credentials, and also change the credentials to major accounts like your bank. Set up alerts too, so you're immediately aware of any unusual activity.
- **Be wary of e-mails:** After a breach, hackers access all kinds of information and may use that to send fraudulent e-mails. Slow down, read carefully and verify requests before taking any action.

CARTOON OF THE MONTH



"OK, who set the thermostat to 33?!"

SCAM OF THE MONTH

Each month we highlight a scam that demonstrates tactics criminals are using RIGHT NOW, to better prepare you when the next scam hits.

Trish had been scrolling through social media when she received the heartbreaking news of a former colleague's passing. She wanted to find a way to pay her respects. It wasn't long before she stumbled upon a Facebook group that seemed to be organizing a live-streamed funeral for the deceased. The page appeared legitimate, featuring heartfelt messages, photos of her colleague, and detailed funeral arrangements. Trish clicked on the link to join the live stream.

Upon entering the group, she was informed that, to access the stream, she would need to pay a small fee. The website was well-designed, and the request for payment didn't seem unusual at first, given the growing trend of online events charging access fees. Without thinking twice, Trish began to enter her credit card information. Only after did she realize that the live stream wasn't real, and she had fallen for a scam.

Did you spot the red flags?

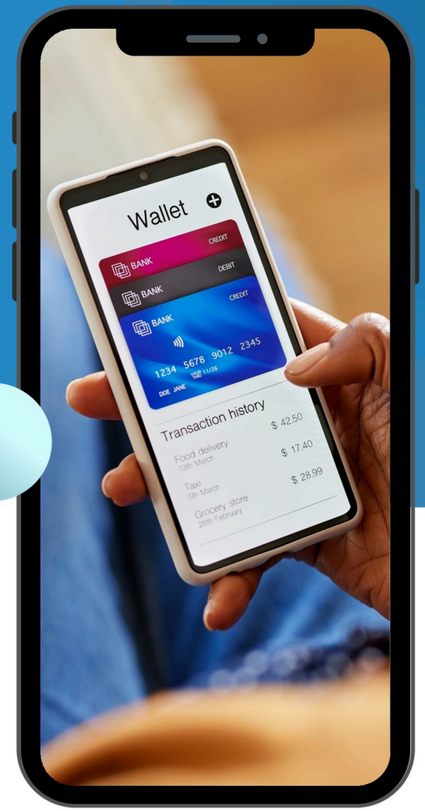
- Trish should have confirmed funeral details through those close to the deceased or through other official channels before searching for information online.
- Never provide personal or financial information unless you are certain of a website's legitimacy.

Check the funeral home's website. Often times the funeral home or family of the deceased will indicate whether the service is being live streamed and provide legitimate links to access the service for free.

Look for warning signs of fake pages and read website reviews. Some scam websites might appear professional at first, but many have subtle red flags, such as poorly written descriptions, fake reviews, or blurry designs.

TIPS AND STRATEGIES FOR FRAUD AWARENESS

Fraud can have devastating consequences financially and reputationally. Let's go over the strategies to protect yourself and your organization.



Preventing

Use caution when online. Do not click on unsolicited links. Be wary of giving out personal information over the phone.

Detecting

Check your bank and credit card statements carefully and often for any signs of fraud. If your contact information or login details have been changed, these could be signs of account compromise.

Resolving

Report signs of fraud to credit bureaus and to any organizations where fraudulent activity has occurred.

PROTECT YOUR DEVICES WITH SECURITY SOFTWARE

PASSION ISN'T ENOUGH:

TIM GROVER EXPLAINS WHY OBSESSION IS KEY TO SUCCESS

Passion is the key to success – that's what many of us have been taught to believe. If you want to be great, you must be passionate. However, Tim Grover believes we've been told wrong.

Tim Grover is a renowned speaker, author and performance coach with over 20 years of experience speaking to businesses, entrepreneurs and leadership teams aiming to be the top in their fields. Known for his work with athletes like Michael Jordan, Kobe Bryant and Dwyane Wade, Grover teaches audiences the mindset of elite professionals so they can apply it to their own success. At a recent industry conference, Grover shared his secret to success: It's not passion that equates to success. It's obsession.

Be Obsessed

Grover draws a clear line between being interested in something and being obsessed with it. "Interest is passive," he explains. If you want to take your business to the next level, you must be all in because when you're obsessed, you pay attention to every tiny detail. As a performance coach, Grover read every injury report for his athletes so he knew how to lace their shoes. He watched hours of video footage and knew every step and landing so he could design training plans. "That's obsession," he says. "That's why they kept me around for such a long time."

Act On Your Passions

"You don't follow your passion," Grover explains. "You act on it. You excel at it." In business, hesitation can lead to missed opportunities. Once a decision is made, you must fully commit to it because excellence is a long game. There will be moments of pressure driving you beyond your comfort zone and moments that feel very isolating. "Excellence creates distance. It creates distance between you, your friends, your enemies, your family, your free time," Grover says. This isolation isn't necessarily negative; it's a byproduct of striving for greatness. It will separate you from everyone who is average – from people who don't understand the behind-the-scenes work it takes to truly succeed in your passion. People will try to pull you down, either out of jealousy or a lack of understanding, but excellence requires a singular focus that many won't understand.

Balance Is A Myth

People often say that successful people need balance. Grover argues that if you try to balance everything – work, life, relationships – while striving for success, you'll be mediocre at all of them. You'll never grow if you're pulled in too many directions. The key to success is ditching balance, focusing on fewer, more important priorities and cutting out distractions. "Everyone has time for what they put first," he explains.

Excellence is a long-term journey that demands obsession, action and a refusal to settle for mediocrity. "Write your own story," Grover says. Put down the self-help books and "look deep down inside yourself and stop looking for everybody else to get you to that next level."

SHINY NEW GADGET OF THE MONTH

DJI Mini 3

If you're looking for a gift that will genuinely impress this holiday, consider the top-rated and budget-friendly DJI Mini 3 drone. It's perfect for any adult who loves tech, photography or exploring new creative hobbies. Its 4K UHD camera captures stunning, crystal-clear aerial shots – ideal for casual flyers and those wanting to take breathtaking photos or videos.

The drone's wind resistance and three-axis gimbal ensure smooth, stable shots, even in less-than-ideal weather. With an extended battery life offering up to 51 minutes of flight (with the optional Intelligent Flight Battery Plus), it provides plenty of time to explore and capture epic landscapes. The DJI Mini 3 is fun and creativity combined, making it an unforgettable gift.

IT Security Tip

- Heads up if you work in HR or process payroll – hackers are very interested in getting you to send employee payroll to the wrong bank accounts.
- Be on high alert for employees asking you to update their banking information.
- Make sure to confirm the change request by phone and do not call any phone numbers in the e-mail that was sent to you.

Bottom line: verbally confirm all requests involving money or sensitive data.

ZOOMING IN ON CYBERSECURITY

A close analysis of computer security and fraud awareness

THIS MONTH'S TOPICS:

As we approach the end of the year, it's more important than ever to stay vigilant against the evolving threats of cybercrime and fraud. Cyber attacks and fraudulent schemes continue to target businesses, often exploiting human error and security vulnerabilities.

In this month's newsletter, we'll focus on actionable tips to secure your computers and protect yourself and your organization against fraud. By staying informed, practicing safe online habits, and fostering a culture of awareness, we can collectively reduce the risks and protect our online environments.

COMPUTER SECURITY

With cyber threats evolving rapidly, every business employee needs to take proactive measures to protect their computer and digital identity. By implementing the latest best practices, you can help ensure that your work devices stay secure and resistant to attacks.

BEST PRACTICES:

- **Keep software up to date.** Outdated programs are often vulnerable to malware, ransomware, and other attacks. It's important to install security updates as soon as they are available to patch vulnerabilities that hackers can exploit. Automatic updates should be enabled to ensure you never miss a crucial update.

- **Remember physical security measures.** To avoid a device being lost or stolen, do not leave devices in your vehicle when traveling. When you are in busy areas, make sure devices are safe in a bag or out of sight. Keep all devices password protected and enable remote wiping. This gives you better control of your sensitive information if a device is stolen.

- **Stay vigilant against malware and scams.** One way to avoid malware is by not clicking on unsolicited links in messages. Verify websites before interacting with them online.