1991 – 2021 30 YEARS OF EXCELLENCE Computer Technologies, Inc.

TECHNOLOGY TIMES

"Insider Tips To Make Your Business Run Faster, Easier And More Profitably"

What's Inside

August 2023

Kim Nielsen, CISSP, CCSA
President &
Chief Technology
Strategist at
Computer
Technologies Inc.
(248) 362-3800

"As a business owner, you don't have time to waste on technical and operational issues. That's where we *shine*! Call us and put an end to your IT problems finally and forever!"

Most Common Brands Faked By Phishers So Far This Year

Cyber-thieves love to use the names of big corporations in their phishing campaigns. If they're spamming large swaths of people, then picking a disguise like Microsoft or LinkedIn increases the odds that more people *use* these services.

Think about it: If you get an urgent message about your car insurance when you don't even own a vehicle, it's pretty obvious that's a scam. That's why cybercriminals focus on and will often choose to impersonate companies that have millions of users.

So…can you guess who's the #1 impersonated brand in 2023?

Top Ten in 2023 So Far

- **Walmart**, accounting for 16% of phishing attacks around the world
- **DHL**, a mail courier service that handles 1.8B deliveries annually and is now impersonated in 13% of global phishing scams
- **Microsoft**, making up 12%
- **LinkedIn** topped the charts toward the end of last year, but now only comes in at 6% of phishing attacks internationally
- **FedEx** comes in at 4.9%, slimly surpassing…
- **Google**, impersonated 4.8% of the time
- **Netflix** fared only barely better at 4%
- **PayPal** scraped just beneath that at 3.5%

What Does All This Mean?
When you look at this list, some of the numbers might surprise you. For instance, did you expect Walmart to top the chart when they were #13 at the tail end of 2022? This is in part because at the tail end of 2022, threat actors perpetuated a scam using Walmart's brand as a

Continued on pg.2

Continued from pg.1

disguise. In their email blast, they "warned" Walmart customers of a potential disruption to their supply chain that may affect shopping and ordering. This false notification was followed by a survey link, which really downloaded infected software.

This is a prime example of why threat actors impersonate big corporations to trick more people at once – rather than **spear-phishing** attacks which are more specific but also more believable as a result.

By mimicking Walmart, the threat actors would have plenty of real customer service emails to comb through and use as a convincing templated

Protect Yourself From Phishing!

The best defensive move that you can make on a daily basis is to ***stay vigilant*** and learn how to recognize new threats and scare tactics as they crop up.

Protecting your and your company's data is a group effort! Even if 99% of the organization flags and reports spam, that 1% can send the whole organization crumbling down. ***Security awareness is a 24/7/365 responsibility.***

If you are notified that your data has been compromised, or may have been exposed in a breach, take immediate action to re-secure your accounts and monitor your credit, systems and profiles for suspicious activity!

Conclusion

Can you tell the difference between a phishing scam and a legitimate message from one of the businesses that you frequent?

Scammers can make fake links, email domains and even webpages that look and feel "real." Spotting inconsistencies in branding, spelling, URLs, old logos and even color schemes can all indicate that a legitimate-seeming email contains more than meets the eye. Be careful communicating with senders outside of your organization, don't click random links or download unknown files, and follow that suspicious feeling in your gut. It's much safer to take a few minutes to verify who you're sending private information to online via the proper, secure channels as outlined in your office's policy.

If you think you've received a suspicious message, **report it** using your email Spam indicator and inform your superiors. They might want to perform their own investigations to evaluate the strength of the organization's entire cybersecurity posture as it stands.

3.4B phishing attacks are spammed out every single day. Take this serious threat, seriously.

Security Corner

Tricks To Avoid Phishing Scams For Mobile Users

Have you taken Security Awareness Training or even passed simulated phishing campaigns at work? Hopefully, you're a little familiar with how to recognize phishing scams on your computer! Unfortunately, those same tips and tricks sometimes work a different way on your mobile device.

Protecting Yourself From Phishing Attacks on Your Phone

Here are some important steps you can take to enhance your mobile security:

1. **Be cautious of suspicious messages**: Exercise caution when you receive unexpected emails, text messages, or social media messages asking for personal or financial information..

2. **Keep your device and apps up to date:** Regularly update your mobile operating system and applications. Software updates often include security patches that address vulnerabilities.

3. **Be cautious with app downloads:** Only download apps from official app stores, such as Google Play Store or Apple App Store. Read reviews and check the developer's information to ensure legitimacy before installing any app.

4. **Be wary of public Wi-Fi networks:** Avoid accessing sensitive information or making financial transactions when connected to public Wi-Fi networks. Public networks may lack proper security measures, making it easier for hackers to intercept your data.

For more information about staying safe while online and other cyber threats, call us at 248-362-3800 or visit: https://tinyurl.com/348cdh53

What Is Zero-Click Malware And How Do You Fight It?

In today's digital landscape, cybersecurity threats continue to evolve. They pose significant risks to individuals and organizations alike. One such threat gaining prominence is zero-click malware. This insidious form of malware requires no user interaction. It can silently compromise devices and networks.

One example of this type of attack happened due to a missed call. That's right, the victim didn't even have to answer. This infamous WhatsApp breach occurred in 2019, and a zero-day exploit enabled it. The missed call triggered a spyware injection into a resource in the device's software.

A more recent threat is a new zero-click hack targeting iOS users. This attack initiates when the user receives a message via iMessage. They don't even need to interact with the message of the malicious code to execute. That code allows a total device takeover.

Below, we will delve into what zero-click malware is. We'll also explore effective strategies to combat this growing menace.

Understanding Zero-Click Malware

Zero-click malware refers to malicious software that can do a specific thing. It can exploit vulnerabilities in an app or system with no interaction from the user. It is unlike traditional malware that requires users to click on a link or download a file.

The Dangers of Zero-Click Malware

Zero-click malware presents a significant threat. This is due to its stealthy nature and ability to bypass security measures. Once it infects a device, it can execute a range of malicious activities. These include:

- Data theft
- Cryptocurrency mining
- Spyware
- Ransomware

This type of malware can affect individuals, businesses, and even critical infrastructure. Attacks can lead to financial losses, data breaches, and reputational damage.

Fighting Zero-Click Malware

To protect against zero-click malware, it is crucial to adopt two things. A proactive and multilayered approach to cybersecurity.

Here are some essential strategies for you to consider:

- ***Keep Software Up to Date –*** Regularly update software, including operating systems, applications, and security patches. This is vital in preventing zero-click malware attacks. Software updates often contain bug fixes and security enhancements.
- ***Educate Users –*** Human error remains a significant factor in successful malware attacks. Educate users about the risks of zero-click malware and promote good cybersecurity practices. This is crucial. Encourage strong password management. As well as act with caution when opening / downloading email attachments or clicking on unfamiliar links.
- ***Conduct Regular Vulnerability Assessments*** – Perform routine vulnerability assessments and penetration testing. Regular testing can help identify weaknesses in systems and applications.
- ***Uninstall Unneeded Applications*** – The more applications on a device, the more vulnerabilities it has. Many users download apps then rarely use them. Yet they remain on their device, vulnerable to an attack.
- ***Only Download Apps from Official App Stores*** – Be careful where you download apps. You should only download from official app stores.

Top 6 Cybersecurity Risks of Remote Work

Remote work has become increasingly popular in recent times. It provides flexibility and convenience for employees. But there are some drawbacks to working outside the office. It's crucial to be aware of the cybersecurity risks that come with remote and hybrid work.

Here are the top cybersecurity risks and tips on how employees and employers can address them.

1.Weak Passwords & Lack of Multi-Factor Authentication: Employers should set up access management systems to automate the authentication process.

2.Unsecured Wi-Fi Networks: To protect company data, remote teams should use a Virtual Private Network

3. Phishing Attacks: To defend against phishing attacks, be cautious when opening emails. Especially those from unknown sources. Avoid clicking on suspicious links. Verify the sender's email address.

4. **Insecure Home Network Devices:** Many remote workers use smart devices that introduce vulnerabilities to their network. Ensure you change the default device passwords and keep them updated with the latest firmware.

5. Data Backup and Recovery: Keep all company files backed up automatically to a central cloud location.

6. **Insufficient Employee Training:** Remote workers should receive proper cybersecurity training. It helps them to understand security risks and best practices. Unfortunately, many companies neglect this aspect of cybersecurity. Organizations should provide comprehensive and ongoing cybersecurity training to remote workers.

Handy Tech Checklist For Home Or Office Moves

Moving can be a chaotic and stressful time. Especially when it comes to handling your valuable technology. Whether you're relocating your home or office, it's essential to take extra care. Both with fragile items and when packing and moving your devices and other tech items.

To help you navigate this process smoothly, we've put together a handy checklist. Use this to help ensure your technology remains safe and sound during the move.

- Back-Up Everything
- Organize and Label Cables
- Pack Devices Carefully
- Remove Ink Cartridges and Batteries
- Take Photos of Cable Connections
- Pack Your Wi-Fi Equipment Separately
- Test Everything After the Move