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

December 2024

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!"

How to Online Shop AND Stay Cyber-Safe

Introduction
When is the last time you bought something via the internet?

2.64 billion people online shop in 2024. With the whole world connected, that's about 1/3 of the global population.

Shopping online can be convenient and fun, but it's also a playground for cybercriminals to lie their way into your wallets and bank accounts. It's important to stay cyber-safe browsing websites that take your home address and financial information. Here are some tips to help you shop more securely!

Tips to Combat Unsafe Shopping
When shopping online, it's crucial to create a secure shopping environment.
For starters, shop on reputable websites. Always look for the padlock icon in the address bar and ensure the site has SSL encryption. To find that out, look for a lock icon near the URL or check if the URL starts with https:// - must have the "s"

If you're unsure about a seller, research that vendor thoroughly by checking their reviews. Stick to well-known and trusted websites; that means to be cautious of misspellings or sites using a different top-level domain.

Once you find a trusted website, use strong passwords to secure your new accounts. Each online account should use a different password, which can be stored in an encrypted Password Manager and retrieved securely with just a click! These extensions can also generate alphanumerically diverse passwords with at least 12

Continued on pg.2

Continued from pg.1

characters, which will greatly increase your accounts' privacy. You should also turn on multi-factor authentication whenever possible, because it will prompt for more verification that the person trying to log into your accounts is truly authorized.

Avoid public Wi-Fi to do your online shopping, too. Don't shop online when connected to public Wi-Fi, as it may not be secure. Instead, rely on your cellular data or a Virtual Private Network.

Finally, it's time to check out with your shopping cart. Protecting your payment and personal information is paramount. Use a credit card or payment service when you pay! They generally offer better fraud protection than debit cards. Still, you should regularly monitor your bank and credit card statements for any unauthorized activity.

Limit the amount of personal information you share during the checkout process to only what is strictly necessary. If the checkout questions look suspicious, take a moment to reassess the seller's validity. When you're buying a nice painting, why does the vendor need too know your date of birth or your mother's maiden name?

If You Fall for an Online Scam

Although we recommend following these tips for the most secure online shopping experience possible, mistakes do happen. Here's how to minimize the damage if you fall victim to an online shopping scam.

Keep your operating system, browser, and antivirus software updated with the latest security patches. This will ensure your devices have the latest security updates, and are hence are more protected from zero-day attacks.

Be vigilant about phishing attempts, which are fraudulent messages designed to steal personal information. Third-party sellers may offer you discounted or scalped concert tickets; you might want to buy a gift on Etsy or a chair on Facebook Marketplace.

Finally, while you're shopping for something within your budget, beware of too-good-to-be-true deals. Extremely low prices or unbelievable offers might be a sign of a scam!

Online purchasing scams are on the rise all around the world. Taking precautions with your online vendors, carefully reviewing shopping e-marketplaces, and vetting sellers through verified customer reviews; all of this will greatly improve your online shopping experience, and save your finances from real trouble.

Happy (and safe) shopping!

Security Corner

Why You Should Hide Apps on Your Phone Screen

From banking details to private messages, our devices often contain data that we want to keep private. One way to enhance your device's security is by hiding apps from your home screen.

Hiding apps can significantly enhance your online privacy. If you have apps that contain sensitive information, such as banking apps, health apps, or private messaging apps, hiding them can protect this data from prying eyes. This is particularly useful in situations where you might need to hand over your phone to someone else temporarily, but don't want them to access your most personal information.

This is also useful when you check your phone in public places. On a public bus, you don't need the person sitting behind you to know too much about the healthcare provider or rent portals you use.

By hiding apps, you simply add an extra layer of security to your online life. It makes it harder for unauthorized users to find and access these apps, thereby reducing the risk of data breaches. This is also especially important if your phone is lost or stolen; while you wipe it remotely clean, the thief will have a harder time finding the banking or email apps they're looking for.

Remember to periodically check the apps you have hidden to ensure they are still necessary to keep out of sight. This helps maintain an organized and secure device, and cleans up some space in your storage too!

For more information about hiding apps, call us at 248-362-3800 or visit: https://tinyurl.com/ydjtmuhn

Watch Out– "Malvertising" Is On The Rise!

There are many types of malware. One of the most common is called "malvertising." It crops up everywhere. You can also see these malicious ads on Google searches.

Two things are making malvertising even more dangerous. One is that hackers use AI to make it very believable. The other is that it's on the rise, according to Malwarebytes. In the fall of 2023, malvertising increased by 42% month over month.

Below, we'll help you understand malvertising and give you tips on identifying and avoiding it.

What Is "Malvertising?"
Malvertising is the use of online ads for malicious activities. One example is when the PlayStation 5 was first released. It was very hard to get, which created the perfect environment for hackers. Several malicious ads cropped up on Google searches. The ads made it look like someone was going to an official site. Instead, they went to copycat sites. Criminals design these sites to steal user credentials and credit card info.

Google attempts to police its ads but hackers can have their ads running for hours or days before they're caught. These ads appear just as any other sponsored search ad. It can also appear on well-known sites that have been hacked or on social media feeds.

Tips for Protecting Yourself from Malicious Online Ads Review URLs Carefully
You might see a slight misspelling in an online ad's URL. Just like phishing, malvertising often relies on copycat websites. Carefully review any links for things that look off.

Visit Websites Directly
A foolproof way to protect yourself is not to click any ads. Instead, go to the brand's website directly. If they truly are having a "big sale," you should see it there.

Use a DNS Filter
A DNS filter protects you from mistaken clicks. It will redirect your browser to a warning page if it detects danger. DNS filters look for warning signs. This can keep you safe even if you accidentally click a malvertising link.

Don't Call Suspicious Ad Phone Numbers
Phishing can also happen offline. Some malicious ads include phone numbers to call. Unsuspecting victims may not realize fake representatives are part of these scams. Seniors are often targeted; they call and reveal personal information to the person on the other end of the line.

Stay away from these ads. If you find yourself on a call, do not reveal any personal data.

Warn Others When You See Malvertising
If you see a suspicious ad, warn others. This helps keep your colleagues, friends, and family more secure. If unsure, do a Google search. You'll often run across scam alerts confirming your suspicion.

It's important arm yourself and others with this kind of knowledge. Foster a culture of cyber-awareness to ensure online security.

8 Steps To Take When You Get A Data Breach Notice

When it happens, you feel powerless. You get an email or letter from a business saying someone breached your data. It happens all too often today. This leaves things like your address, SSN, and credit card details exposed to thieves.

A business getting hacked is something you have little control over, but you can take important steps afterward. We've outlined the most important things to do. These steps can help you mitigate the financial losses.

1. Change your passwords.
2. Enable multifactor authentication (MFA).
3. Check your bank accounts.
4. Carefully review the breach notification.
5. Freeze your credit.
6. Get good cybersecurity protections.
7. Be on the lookout for phishing scams.
8. Make sure to update software & systems.

5 New Trends From A Study On The State Of AI At Work

Microsoft and LinkedIn released a joint report providing valuable insights into the current state of AI in the workplace. The study sheds light on how AI is transforming the way we work. Here are the main trends:

1. Employees want and expect AI at work. AI helps them do certain things faster.
2. AI skills are becoming more in demand. Companies are seeking AI-skilled staff.
3. The evolving role of employees using AI. Companies can benefit from their AI power users.
4. Things can get messy fast without a plan. It's the "Wild West" without a use policy in place.
5. For the ethical considerations and trust in AI, there must be clear communications to employees and customers

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

Use These Best Practices For Event Logging

To stand ahead of threats, a strong cybersecurity strategy is essential. One crucial component of this strategy is event logging: the act of tracking all events that happen within your IT systems.

It is most effective when you follow best practices:

- **Log what matters most**. These are events that can reveal security breaches.
- **Centralize your logs**. Use a SIEM; it gathers logs in one place.
- **Ensure logs are tamperproof**. Protect your logs for an accurate record of events even if a breach occurs.
- **Establish log retention policies**. Strike the right balance with retention.
- **Check logs regularly**. Event logging is only as good as your ability to use it.