TECHNICAL FRAMEWORK
INFORMATION TECHNOLOGY SERVICES

(970) 372-4940
info@techframework.com
https://techframework.com

“Malvertising” is on the Rise!

TECH INSIDER

January 2025

Corporate

Personal & Home-Office

CORPORATE

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,

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.

Do Not Log in After Clicking an Ad

Malvertising will often land you on a copycat site. The login page may look identical to the real thing. One of the things phishers are trying to steal is login credentials.

If you click an ad, do not input your login credentials on the site, even if the site looks legitimate. Go to the brand’s site in a different browser tab.

Don’t Call Suspicious Ad Phone Numbers

Phishing can also happen offline. Some malicious ads include phone 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 details.

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 wellknown 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. Just don't click those links and go to the source directly.

Use a DNS Filter

A DNS filter protects you from mistaken clicks.

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.

Don't Download Directly from Ads

"Get a free copy of MS Word" or "Get a Free PC Cleaner." These are common malvertising scams. They try to entice you into clicking a download link. It's often for a popular program or freebie. The link actually injects your system with malware to do further damage.

A direct download link is likely a scam. Only download from websites you trust.

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 safety and better online security.

DALL-E prompt: A sleek, compact biometric smart safe device called TROVA GO, made of lightweight aluminum alloy, placed on a clean, minimalist surface. The device is modern and elegant, with soft curves and a matte finish. Next to it is a smartphone displaying the TROVA app interface, showcasing keyless Bluetooth-enabled access.

PERSONAL & HOME-OFFICE

TROVA GO

TROVA GO is a personal biometric smart safe that puts mobile privacy and security into the palm of your hand.

It's a small device designed to store a few key items that require privacy and protection.

TROVA app offers keyless, no combo & hassle-free access. It's paired with wireless connectivity via Bluetooth for smart notifications.

It is crafted from sturdy yet lightweight Aluminum Alloy for durability.

CORPORATE

Smart Windows 11 Settings for Productivity

The newest Windows OS is fast gaining ground on Windows 10. As of August 2024, Windows 11 had over 31% of the Windows market share. That is bound to increase fast as Windows 10 retires in 2025.
Already upgraded to the new operating system or planning to soon? You'll love these tips on optimizing your Windows 11 experience and transforming your daily workflow.

1. Start Menu Customization

● Pin Frequently Used Apps: Right-click on any app and select "Pin to Start." to keep your most-used applications just a click away.
● Organize into Folders: Drag and drop apps on top of eachother to create folders.

2. Virtual Desktops

● Create a New Desktop: Click on the Task View button or press Win + Tab. Click on "New Desktop" to create a new virtual space.
● Switch Between Desktops: Use Ctrl + Win + Left/Right Arrow to switch between desktops.

3. Snap Layouts and Snap Groups

● Use Snap Layouts: Hover over the maximize button on any window to see available snap layouts. Choose a layout to snap the window into place.
● Create Snap Groups: Snap windows into a layout. Windows 11 remembers the group. Hover over the taskbar icons to see and restore the snap group.

4. Focus Assist

● Enable Focus Assist: Search "Focus" from the taskbar and click Focus Settings. Choose your options and click to start a session.
● Set Automatic Rules: Configure automatic rules to enable Focus Assist during specific times. For example, when duplicating your display or when playing a game.

5. Taskbar Customization

● Pin Apps to Taskbar: Rightclick on any app and select "Pin to taskbar" for quick access.
● Adjust Taskbar Settings: Right-click on the taskbar and choose "Taskbar settings" to customize taskbar behaviors like hiding it in desktop mode or showing badges on taskbar buttons.

6. Keyboard Shortcuts

● Win + E: Open File Explorer.
● Win + I: Open Settings.
● Win + D: Show or hide the desktop.
● Win + L: Lock your PC.
● Alt + Tab: Switch between open apps.

7. Power and Battery Settings

● Adjust Power Mode: Go to Settings > System > Power & battery to choose a power mode that works best for you.
● Battery Saver: Enable Battery Saver to extend battery life. Use it when your device is running low or you're away from power for an extended time.

8. Storage Sense

● Enable Storage Sense: Go to Settings > System > Storage. Turn on Storage Sense and configure it to run automatically.
● Configure Cleanup Schedules: Set up schedules for several tasks to clean up your storage.

Looking for more IT tips? Our team of tech experts has many other productivity tips to share. Don't hesitate to reach out to us for more productivity enhancers.

DALL-E prompt: An office desk with a laptop displaying 'Password Manager' and a glowing lock icon. The screen shows connected account icons (email, banking, social media) with secure lines. The setting includes a coffee cup, notebook, and soft natural light, emphasizing security with vibrant neon blue and green tech tones.

CORPORATE

How Password Managers Protect Your Accounts

A password manager keeps all your passwords in one place. Think of it as a digital safe for your login information.

You only need to remember one password, the master password. This master password lets you access all your other passwords.

Types of Password Managers

- Apps you download on your phone or computer
- Tools that work in your web browser
- Some offer both options

Why Use a Password Manager?

- It Helps You Create Strong Passwords. Password managers generate long, random passwords that are hard to crack.

- It Remembers Your Passwords. With a password manager, you don't need to memorize many passwords. The tool does this for you.

- It Keeps Your Passwords Safe. Password managers use high-level security to protect your data. Even if someone hacks the password manager company, they can't read your information.

Features of Password Managers

- Password Generation: Good password managers can create tough, unique passwords for you.

- Auto-Fill: Many password managers can fill in your login information on websites. This saves time and avoids typos.

- Secure Notes: Some password managers let you store credit card numbers or important documents.

- Password Sharing: Some tools let you share passwords safely with family or coworkers.

How to Choose a Password Manager

- Find one with strong encryption and two-factor authentication.
- The manager should be easy for you to understand and use.
- Make sure it works on all your devices.
- Research the features you want and the price you can afford.

Consider using a password manager today to improve your online security.

If you need help choosing or setting up a password manager, contact us today.

PERSONAL & HOME-OFFICE

How is Your Cyber Hygiene? Essential Tips For 2025

- Improve your passwords. Passwords are like keys to your online home.

- Update your software. Updating your software is like getting a flu shot.

- Implement two factor authentication. It's like putting two locks on your door.

- Be careful on public Wi-Fi. It's like yelling in a crowded place.

- Identify phishing scams. It's like a fake fisherman trying to catch you.

- Back up your data. It's like making copies of your important papers.

- Review privacy settings. Your privacy settings are like curtains on your windows.

- Teach your family about cybersecurity. This is for everyone in

PERSONAL & HOME-OFFICE

Innovative Solutions to IoT Device Security

The Internet of Things is growing day by day. More devices are connecting to the internet. And with that growthcomes new security risks.

Here are some new ways to keep your IoT devices safe.

- Use strong passwords. Always change the default password.
- Always update software. This closes the security gaps in the software.
- Encrypt your data. This scrambles data so others cannot read it.
- Develop an IoT security policy. Establish regulations relating to the use and security of IoT devices.
- Implement network segmentation. Isolate the IoT devices from other networks.
- Do research before buying. Choose devices from companies that take security seriously.
- Secure your home network. Enable network encryption.
- Think twice about what you connect. Only connect devices you

your family. It's like teaching kids to look both ways.

need.

CORPORATE

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. Freeze your credit.
5. Carefully review the breach notification.
6. Get good cybersecurity protections.
7. Be on the lookout for phishing scams.
8. Make sure to update software & systems.

Managed services can keep you protected at work and home. Let's improve your device security.

Technical Framework maintains an **A+** rating with the **BBB** A+ BBB

FORT COLLINS AREA CHAMBER OF COMMERCE

GREELEY AREA CHAMBER OF COMMERCE