ISSUE 002
December 2024
Ave Maria, Florida

Stilwell Support
Expert Support with Wallet-Friendly Solutions.

TECH TALK

"Insider Tips to Make Your Business Run Faster, Easier and More Profitable"

INSIDE THIS ISSUE:

We love technology and we love helping people.

Give me a call today for a quick (non-salesy) chat to find out whether my team and I can help you better secure your data and get more out of your existing technology!

- **John Stilwell**
Founder & CEO

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

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.

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 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

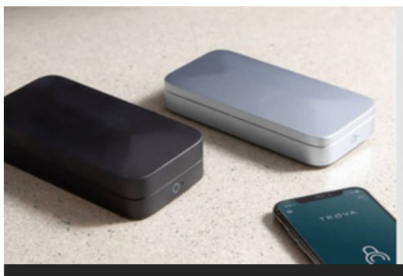
"Get a free copy of MS Word" or "Get a Free PC Cleaner." Theseare common malvertising scams. They try to entice you into clicking a download link. It's often for a popular program or freebie. The link actually injects your system with malware to do further damage.

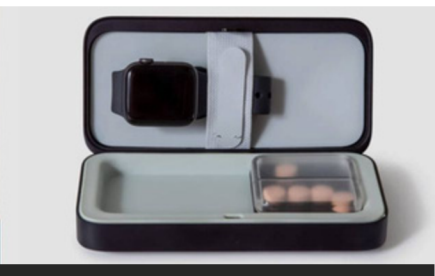
A direct download link is likely a scam. Only download from websites you trust.

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.





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.

ISSUE 002
December 2024
Ave Maria, Florida

Stilwell Support
Expert Support with Wallet-Friendly Solutions.

SMART WINDOWS 11 SETTINGS FOR PRODUCTIVITY

The newest Windows OS is fast gaining ground on Windows10. As of August2024, 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 each other 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: Right- click 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.

HOW CAN SMALL BUSINESSES EMBRACE THE CASHLESS REVOLUTION?

The world has adopted payment wallets, and people expect businesses to accept them. These include Apple Pay, Google Pay, PayPal and more.

Small businesses need to keep pace to meet customer expectations. People want fast, easy, and secure payment options. You can easily lose business if people can't pay the way they like.

Key Steps to Go Cashless

Step 1: Choose the Right Payment Solutions.
Select payment methods that align with your customers' preferences. Do your research by sending customers a survey. Start with the three most popular methods. You can then branch out from there. Make sure to check transaction fees.

Step 2: Educate Your Customers.
Let customers know about your new cashless options. Offer incentives to encourage adoption. Get the word out over social media and through any mailing lists you have.

Step 3: Strengthen Security Measures.
Protect your business and customers from fraud with robust security measures. Make sure your point-of-sale devices are on a secure network.

Step 4: Watch Transactions and Customer Trends.
A nice thing about cashless systems is that they generate helpful data. Analyze data to optimize your payment processes and identify opportunities.

Step 5. Plan for the Future.
Stay updated on payment trends and be prepared to adapt as needed. Add new ones that seem to be picking up steam. Continue to survey customers on their favorite payment options.
You can often get your best ideas from customer feedback.

The cashless revolution is here. As your trusted IT partner, we're here to support you every step of the way. Let's make the transition to cashless payments a seamless one for your business.

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 identified:

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 about how AI is used.

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 and compliance risks.
• **Centralize your logs.**
Use a SIEM; it gathers logs in one place.
• **Ensure logs are tamper- proof.**
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.

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 look out 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.

TECHNOLOGY TRIVIA TIME

The question this month is:

What is the first search engine on the internet?

Last month's answer was
Deep Blue.