Connection

January 2024

We believe that experienced, reputable, and fast responding IT support should be the standard!

Our Services:

- Data Backup & Recovery
- Managed Services
- IT Consulting
- Network Security
- Cloud Computing
- Remote IT Services
- Cyber Security Training
- Mobile Device Management
- VoIP Phones

Let's get social!

Instagram:
computer_services_unlimited

Facebook:
Computer Services Unlimited Inc.

LinkedIn:
Computer Services Unlimited Inc.

Phone:
(703) 968-2600

Digital Newsletter:
www.csuinc.com/news

Warning About New Devices After the Holidays

The holiday season often ushers in a wave of new devices—smartphones, laptops, and tablets—that employees are eager to use. While these gifts are exciting, they can also pose significant risks to your company's security when connected to your network. Welcome to the world of BYOD (Bring Your Own Device).

Although employees are enthusiastic about using their new gadgets for work, these personal devices can introduce serious security threats, such as malware, ransomware, and spyware, especially if they contain unsanctioned apps.

(continued on page 2)

Key BYOD Security Risks

BYOD can create security vulnerabilities since personal devices often lack the security controls of company-issued equipment. The main risks include:

- **Lost or Stolen Devices**:
  Personal devices are more likely to be misplaced, exposing sensitive data to unauthorized access.
- **Malware & Unauthorized Apps**:
  Employees might unknowingly download malicious software or use unapproved apps that compromise company security.
- **Unsecured Networks**:
  Public Wi-Fi networks can be exploited by hackers, putting company data at risk.
- **Data Leakage**:
  Employees might share sensitive information through unsecured channels or malicious third-party apps.
- **Unclear Security Policies**:
  Employees may not be aware of security risks and could bypass policies, exposing the network to threats.

A well-defined BYOD policy is essential, regardless of your company's size.

Note: We aren't lawyers, but we can help you outline a BYOD policy tailored to your business. However, it's important to have your attorney review the policy to ensure legal compliance.

Tips for a Strong BYOD Policy

- **Regular Device Audits**
  Conduct regular audits to ensure devices meet security standards, including the latest OS updates and security software.
- **Mandatory Security Software**
  Require employees to install up-to-date antivirus software, firewalls, and anti-malware tools on their devices.
- **Mobile Device Management (MDM)**
  Use MDM software to enforce security standards and remotely lock or wipe devices if they're lost or stolen.
- **VPNs and Encrypted Wi-Fi**
  Encourage the use of VPNs for secure connections when accessing company resources remotely and ensure employees connect to encrypted Wi-Fi networks.
- **Clear Employee Expectations**
  Set clear guidelines on how personal devices should be used for work and educate employees on their responsibilities to protect company data.

Instagram: computer_services_unlimited
Facebook: Computer Services Unlimited Inc.
Phone: (703) 968-2600

- **Strong Authentication**
  Implement multi-factor authentication (MFA) or biometric measures to ensure only authorized individuals access company resources.
- **Least Privilege Access Control**
  Limit access to company resources based on job requirements, reducing the potential impact of a security breach.

If your company operates in a regulated industry (Finance, Healthcare, Law, etc.), a BYOD policy is crucial for compliance with regulations like HIPAA, GDPR, or SOC 2. A strong policy helps reduce data breach risks and ensures compliance.

Need help reviewing or creating a Bring Your Own Device policy? Reach out, and we can assist you in ensuring your business stays secure.

Tech Giggles!

What's a computer's favorite snack?

...

Micro-chips!

DO YOU REALLY NEED DARK WEB MONITORING?

Dark web monitoring looks for your information on the dark web. It can find stolen passwords or credit card numbers. This helps you know if someone stole your data.

But is dark web monitoring really necessary? Here are the most important benefits to consider:

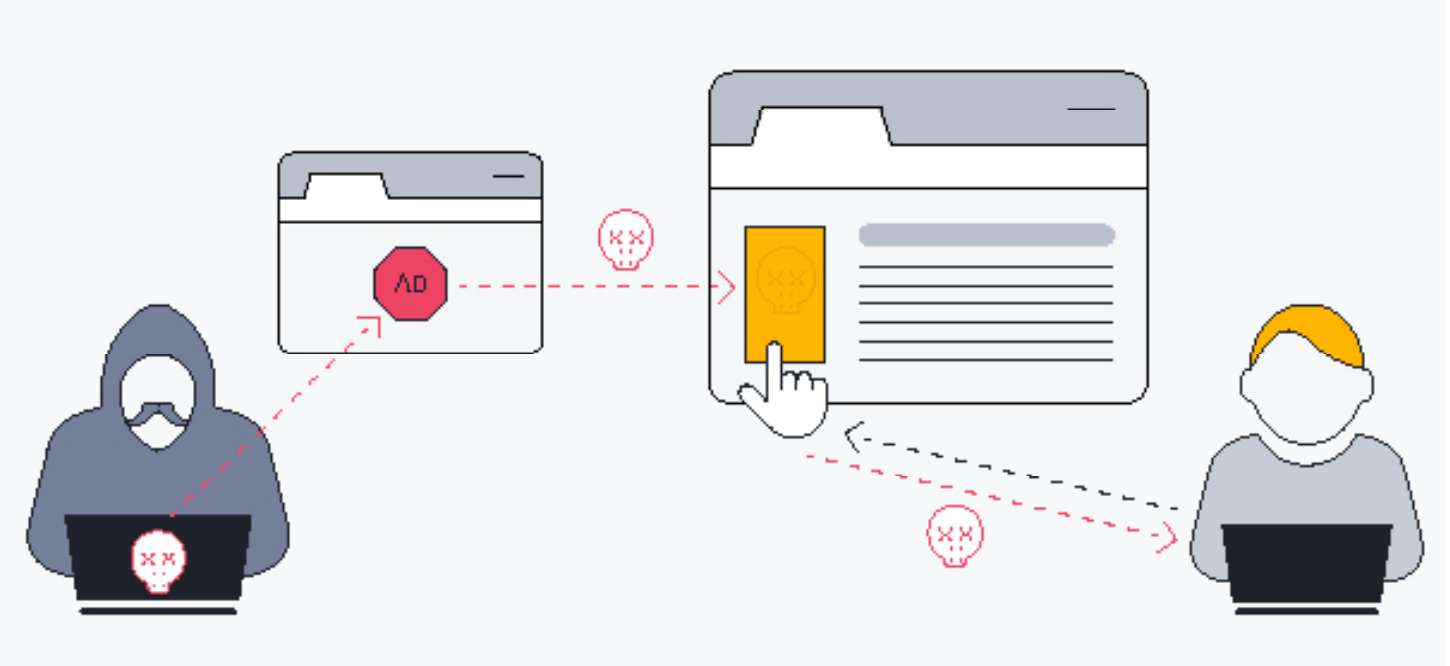
IDENTITY AND BUSINESS PROTECTION. It helps you know if someone stole your personal or business data. You can then change passwords and protect yourself.

AI MONITORING TO SPOT PATTERNS THAT PEOPLE MIGHT MISS. AI helps them search faster and better.

REAL-TIME ALERTS WHEN YOUR INFORMATION IS STOLEN. The tools send an alert right away when they find your information.

PROTECTION FOR PASSWORDS, CREDIT CARD NUMBERS, SOCIAL SECURITY NUMBERS, AND MORE. This enables you take quick, specific actions.

Dark web monitoring is an easy way to protect your information. It watches when you can't. If you want to stay safe online, it's a good tool to have.



Watch Out for "Malvertising"

There are many types of malware, but one of the most common and concerning is called "malvertising." It's cropping up everywhere, even in places like Google searches. What makes malvertising even more dangerous? Two key factors: hackers are using AI to make it incredibly convincing, and its frequency is skyrocketing. According to Malwarebytes, in the fall of 2023, malvertising increased by 42% month over month.

In this article, we'll explain what malvertising is, how to identify it, and offer tips for avoiding it.

What Is "Malvertising?"

Malvertising involves the use of online ads for malicious activities. One prominent example was during the release of the PlayStation 5. As demand soared and availability dwindled, hackers seized the opportunity. Malicious ads appeared in Google searches, misleading users into visiting copycat sites. These sites were designed to steal personal information, such as user credentials and credit card details.

While Google attempts to monitor and police these ads, hackers often get theirs through before they're caught—sometimes running for hours or days. These deceptive ads can appear just like any other sponsored search results and may also show up on hacked, well-known websites or even social media feeds.

Tips for Protecting Yourself from Malicious Online Ads

1. Review URLs Carefully

Look out for small misspellings or strange characters in an ad's URL. Similar to phishing attacks, malvertising often relies on imitating trusted websites. Double-check any links for signs of inconsistency.

2. Visit Websites Directly

A simple way to protect yourself is to avoid clicking ads altogether. Instead, go directly to the brand's official website to check for promotions or sales. If there is a "big sale," you should find details directly on the site.

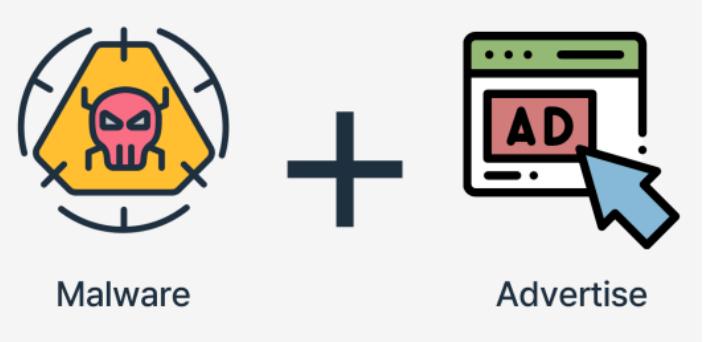
Instagram: computer_services_unlimited
Facebook: Computer Services Unlimited Inc.
Phone: (703) 968-2600

3. Use a DNS Filter
A DNS filter helps protect you from accidental clicks on malicious links. If a suspicious link is clicked, a DNS filter can redirect you to a warning page to keep you safe from malvertising.

4. Do Not Log In After Clicking an Ad
Malvertising can land you on a fraudulent site that mimics a legitimate login page. Be cautious: never enter your login details after clicking an ad, even if the site looks real. Open a new tab and go directly to the brand's website.

5. Don't Call Suspicious Ad Phone Numbers
Some malvertising scams include phone numbers to call for "assistance." These fake representatives are often scammers, particularly targeting vulnerable groups like seniors. Never share personal information over the phone if you suspect the ad is a scam.

6. Don't Download Directly from Ads
Beware of ads promising "free downloads" for popular software like MS Word or PC cleaners. These are common traps used to deliver malware onto your device. Only download files from trusted websites, never from ads.



7. Warn Others When You See Malvertising
If you spot a suspicious ad, alert your colleagues, friends, and family. Sharing this information helps others stay secure online. A quick Google search often uncovers scam alerts confirming the ad's malicious nature.

Stay alert, educate yourself, and promote a culture of cyber-awareness. This knowledge can help ensure safer online experiences and better security for everyone.

Gadget of the Month!

TickTime Cube

Ticktime Cube is your ultimate time manager to boost your efficiency and productivity.

The TickTime Cube is a single task countdown timer with a built-in Pomodoro mode. Just flip it and the timer will restart for you.

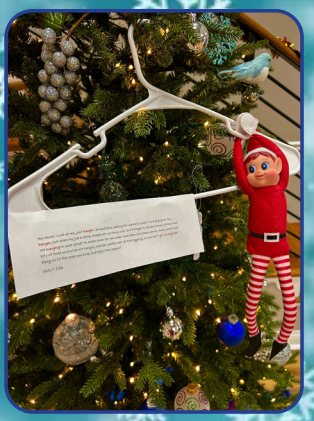
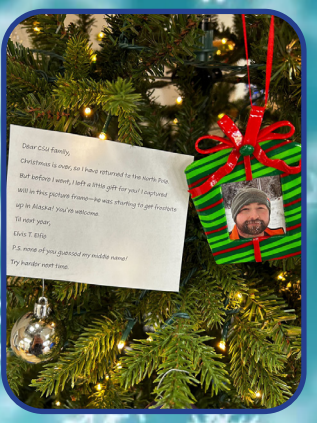
The timer comes with a selection of preset countdown times, but you can also set a custom time of 99 minutes and 59 seconds or less or use the stopwatch feature to count up.

It's a fun way to keep track of your time.

$31.99 on Amazon!

What's NEW at CSU?



ELF SHENANIGANS

Santa sent Elvis T. Elfie to CSU! He gathered up an army of minions, got his collar and hat piece torn off by a ferocious beast (a puppy), caught a mouse, hung on our Christmas tree, and trapped Will in an ornament as a gift to us for Christmas!





White Elephant

The CSU team had an absolute blast playing White Elephant! Poor Chuck had two items stolen from him—Caitlyn swiped the back massager, and Paola took the remote scrolling ring. In retaliation, Chuck stole the Nerf gun from Melvin. That left Melvin with popcorn treats and... a whole bunch of gift bags? Looks like someone had an excess of gift bags to unload!

Instagram: computer_services_unlimited
Facebook: Computer Services Unlimited Inc.
Phone: (703) 968-2600

JANUARY BIRTHDAYS!

The woman who runs the show is a January baby! Michelle is turning 21 again! Thank you for all you do for CSU. We wish you a very happy birthday and a successful year ahead!

Another year another wrinkle! Your hard work makes a huge impact for CSU, and your sense of humor makes every day brighter. Wishing you a fantastic birthday, Melvin!

Twin Day!

We had a couple of twins in the office for Twin Day! Michelle and Caitlyn twinned in a plum shirts and blue jeans. Paola and Melvin twinned in sweaters, vests, and black pants.

Ugly Sweaters

Ugly sweater day! Who do you think had the ugliest sweater?