DTS DanTech Services
Computers under control!™

Technology Times October 2024 Issue

"With over 20 years of experience providing remote support to clients that rely on technology, I know what it takes to deliver business continuity. Add to that another 20 years of support in the service industry you'll not find another company that takes customer service to heart as I do. Find out for your business what a difference it makes. "

What's Inside:

October is Cybersecurity Awareness Month

Cybersecurity Awareness Month has arrived, reminding us that businesses and organizations of all sizes are at risk of being hacked in today's digital landscape. This reality is a part of our modern lives, yet many companies and individuals fail to adequately prepare for breaches that could have serious repercussions on their operations, brand image, reputation, and revenue.

Cyberattacks are occurring more frequently and with increasing sophistication, affecting all types of companies, particularly small and medium-sized enterprises. A recent study by Accenture revealed that 43% of cyberattacks target small businesses, but only 14% of those businesses are equipped to defend against them.

As internet connectivity expands, the frequency of attacks by criminal hackers is rising. They are leveraging machine learning to identify vulnerabilities and automate their attacks, resulting in faster, smarter, and more devastating breaches. Additionally, hackers often utilize tools available on the Dark Web as part of their operational strategies. Threat actors comprise a range of entities, including state-sponsored groups, criminal organizations, and hacktivists.

It's important to note that hackers do not always need the latest software to succeed. Often, they target the most vulnerable victims at opportune moments. The increasing complexity of socially engineered threats, particularly deep fakes, presents a significant challenge for organizations trying to defend themselves.

- Continued on page 3

Beware of Cybercrime even during your Google searches

Malvertising is a tactic used by hackers for phishing purposes or to install malware on users' computers. In malvertising, hackers use online advertising for these malicious purposes.

Both consumers and corporate employees are targeted through ads that appear on mainstream websites or through sponsored ads found during routine web searches. Some of these ads will only infect users who click on them, but others can infect users who just visit the site.

Recent incidents include Google ads targeting Lowe's employees, which directed them to a phishing website, "myloveslife.net," containing a subtle misspelling of the company name. The website did contain a genuine Lowe's logo. IT security experts say the brand name and logo are often enough to convince employees the site is real.

Malvertising has been around for a while, but these days, cybercriminals are making the ads look so realistic that it's easy to be fooled. Tactics to avoid such hacking attempts include:

- Keeping your systems updated.
- Using anti-malware software, ad blockers and privacy browsers.
- Avoiding clicking on the sponsored ad directly, but go to the specific site instead.
- Educating friends and family about the risks and signs of malvertising.

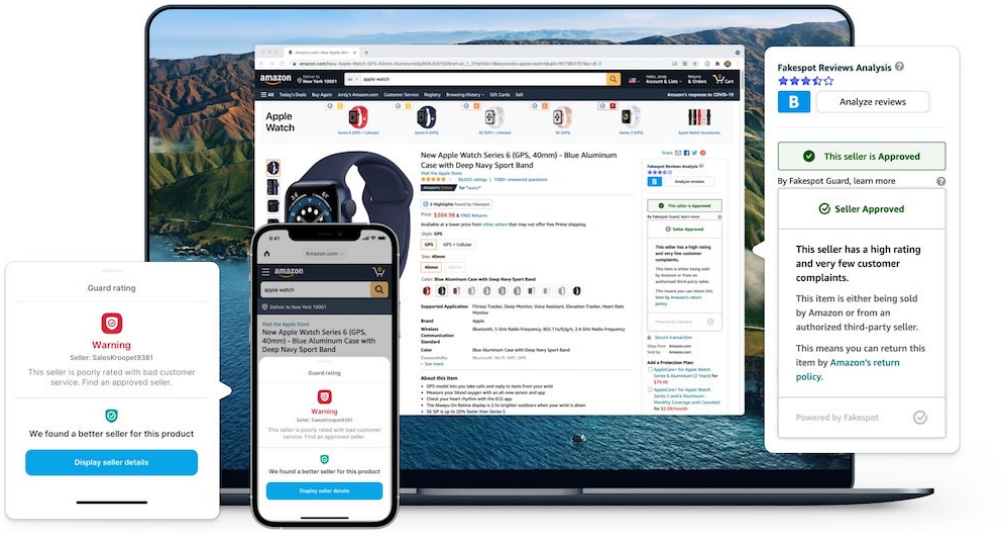
Fake product reviews are common. Learn how to spot them

With the AI boom, distinguishing genuine reviews from fake ones can be challenging. Here, we offer several tips to feel more confident about your purchases based on the online reviews you read.

One tip is to know what you're looking for. Fake reviews often use excessively positive or generic language and lack specific details about the product or service. Be cautious if you read a review that offers a high rating with no justification.

If a product has received many positive reviews within a short period, that may also be a sign the reviews are fraudulent. Genuine reviews often include photos or videos of the products. Ensure these images look authentic and relevant to the product in question.

Amazon also helps its shoppers by marking reviews from legitimate buyers with a "Verified purchase" label. Investigate further by looking into profiles of these



reviewers. Legitimate reviewers will usually have a mix of positive and negative reviews. Be wary of reviews that are too brief or overly detailed.

If you're still unsure, rely on tools like **Fakespot** or **ReviewMeta**, which help you identify suspicious patterns and provide a reliability score for these reviews.

Fakespot is a tool that evaluates the reliability of product pages on major e-commerce sites (such as Walmart, Sephora, and eBay). It analyzes the language used in reviews, product reviews, and purchase history to determine the trustworthiness. Enter a product page URL into the **Fakespot Analyzer** to get a reliability grade and a product rating.

Similarly, users can paste an Amazon URL into a **ReviewMeta** search bar, and the website analyzes the reviews and eliminates those it deems unreliable. It provides an adjusted rating based on various criteria.

ReviewMeta also offers a detailed report card and breakdown of the factors used in that adjusted rating.

The importance of informal leaders in a cybersecurity team

While formal management is essential, informal leaders also play a crucial role by guiding and inspiring their team members.

Recognized by their coworkers for their reliability, encouragement, and ability to lead projects successfully, these individuals naturally command respect and influence within their teams.

Their ability to foster unity and a sense of purpose is invaluable, especially in high-stress situations. The presence of informal leaders can strengthen the team's ability to develop innovative solutions, increasing the likelihood of success.

There are many benefits of having informal leaders. They help boost morale and collaboration, keeping peers engaged and motivated, particularly during stressful and challenging situations.

By supporting their fellow team members, informal leaders contribute to a stronger, more cohesive team. They often promote a culture of continuous learning and improvement, which is crucial in a field that must stay ahead of ever-evolving cyberthreats.

The role of informal leaders is critical to helping teams navigate the complexities of the dynamic world of cybersecurity.

Becoming an informal leader can also help you develop leadership skills and build stronger relationships with peers, ultimately leading to the teams' success and enhancing your personal and professional growth.

" Cybersecurity Awareness Month"- continued from page 1

Cybersecurity Awareness Promotes Effective Risk Management

While everyone is susceptible to cyberattacks, steps can be taken to mitigate risks. The initial measure is to develop a risk management plan and maintain vigilance. A robust risk management strategy must encompass data privacy, application security, cyber vulnerability assessments, network access configurations, best practices for cyber hygiene, usage policies, permissions, and ongoing education and training.

This strategy involves people, processes, and tools. In essence, cyber-awareness means staying alert, identifying gaps, assessing weaknesses, and implementing protective measures for individuals or organizations.

In our increasingly volatile digital environment, a security plan for managing risk must be both comprehensive and adaptable to emerging threats.

Four Easy Ways to Stay Safe Online

Let's work together to build a safer digital world. We can increase our online safety through four simple actions, and whether at home, work or school, these tips make us more secure when connected. Take time to discuss them with family, friends, employees and your community so we can all become safer online!

Recognize & Report Phishing

Be cautious of unsolicited messages asking for personal information. Avoid sharing sensitive information or credentials with unknown sources. Report phishing attempts and delete the message.

Use Strong Passwords

Strong passwords are long, random, unique and include all four character types (uppercase, lowercase, numbers and symbols). Password managers are a powerful tool to help you create strong passwords for each of your accounts.

Turn On MFA

You need more than a password to protect your online accounts and enabling MFA makes you significantly less likely to get hacked. Enable MFA on all your online accounts that offer it, especially email, social media and financial accounts.

Update Software

Ensuring your software is up to date is the best way to make sure you have the latest security patches and updates on your devices. Regularly check for updates if automatic updates are not available.

Shiny Gadget of The Month

Ember Temperature Control Smart Mug 2, 10 Oz, App-Controlled Heated Coffee Mug with 80 Min Battery Life and Improved Design, Black

- Ember Coffee Mug with Longer Lasting Battery: Our updated smart coffee mug's extended battery life keeps your drink at your preferred temperature (between 120°F - 145°F) for up to 80 minutes on a full charge or all day on its redesigned charging coaster

- Smart With or Without App: Pair this temperature control mug with the Ember app to set the temperature, customize presets and more;

- Our self-heating coffee mug is also functional without the app and remembers your last-used temperature (135°F out of box)

- Auto Sleep: Our heated coffee mug intelligently senses when to turn on and off; The mug enters sleep mode when empty or after 2 hours of inactivity; Ember wakes up when it senses movement or liquid

- Hand Wash Only: An updated scratch-resistant coating is safe to hand wash; Ember Mug 2 is IPX7 rated and fully submersible up to 1 meter deep.

- Perfect Gift for a Life Well Sipped: Whether self-gifted or given to another, there's no better way to share warmth than a favorite drink at just the right temperature every time.

Zero Trust Architecture Explained

Zero trust is a cybersecurity strategy wherein security policy is applied based on context established through least-privileged access controls and strict user authentication—not assumed trust. A well-tuned zero trust architecture leads to simpler network infrastructure, a better user experience, and improved cyberthreat defense.

A zero trust architecture follows the maxim **"never trust, always verify."** This guiding principle has been in place since John Kindervag, then at Forrester Research, coined the term. A zero trust architecture enforces access policies based on context—including the user's role and location, their device, and the data they are requesting—to block inappropriate access and lateral movement throughout an environment.

Establishing a zero trust architecture requires visibility and control over the environment's users and traffic, including that which is encrypted; monitoring and verification of traffic between parts of the environment; and strong multifactor authentication (MFA) methods beyond passwords, such as biometrics or one-time codes.

Critically, in a zero trust architecture, a resource's network location isn't the biggest factor in its security posture anymore. Instead of rigid network segmentation, your data, workflows, services, and such are protected by software-defined micro-segmentation, enabling you to keep them secure anywhere, whether in your data center or in distributed hybrid and multi-cloud environments.

What are the Core Principles of the Zero Trust Model?

Zero trust is about more than user identity, segmentation, and secure access. It's a strategy upon which to build a cybersecurity ecosystem. At its core are three tenets:

- **Terminate every connection:** Technologies like firewalls use a “passthrough” approach, inspecting files as they are delivered. If a malicious file is detected, alerts are often too late. An effective zero trust solution terminates every connection to allow an inline proxy architecture to inspect all traffic, including encrypted traffic, in real time—before it reaches its destination—to prevent ransomware, malware, and more.

- **Protect data using granular context-based policies:** Zero trust policies verify access requests and rights based on context, including user identity, device, location, type of content, and the application being requested. Policies are adaptive, so user access privileges are continually reassessed as context changes.

- **Reduce risk by eliminating the attack surface:** With a zero trust approach, users connect directly to the apps and resources they need, never to networks (see ZTNA). Direct user-to-app and app-to-app connections eliminate the risk of lateral movement and prevent compromised devices from infecting other resources. Plus, users and apps are invisible to the internet, so they can’t be discovered or attacked.