THE CYBERSIDE BRIEF

Over 20 Years of Insider Wisdom on IT Defense for Your Business Prosperity and Security

INSIDE THIS ISSUE

6 SHOPPING SCAMS AND HOW TO AVOID THEM

It's October, which means the biggest online shopping day of the YEAR is just weeks away: Cyber Monday. Unfortunately, it's also open season for cybercriminals. Because preparation is the best prevention, we're covering the six most common shopping scams this time of year and how to avoid them.

It's Open Season For Shopping Scams

Thanks to cybercriminals, what should be a season of festive shopping is now dangerous for consumers. According to the Federal Trade Commission, shopping scams were the second-worst type of scam in the US in 2023. And online scams are at their worst during the holidays. According to TransUnion's 2022 Global Digital Fraud Trends report, there was a 127% increase in daily fraud attempts between November 24 and 28 compared to January 1 through November 23.

Due to the high volume of shopping activity during the holiday season, cybercriminals don't have to work hard to find potential victims. But it's not simply volume that contributes to the rise in attacks; consumers take more risks during the holiday season. According to Norton's 2022 Cyber Safety Insights Report, nearly one in three adults (32%) worldwide admitted to taking more risks with online shopping closer to the holidays. Last-minute shopping pressure or excitement around scoring big deals results in common mistakes, including clicking on unverified links, using public WiFi for transactions and ignoring website security red flags.

continued on page 2...

This monthly publication is provided courtesy of Patrick Birt, President of AdRem Systems Corporation.

...continued from cover

Cybercriminals expect shoppers to make mistakes, and they have tried-and-true tactics for stealing your money. Watch out for these six scams that appear this time of year, and protect yourself this holiday season.

6 Common Scams During Black Friday And Cyber Monday And How To Avoid Them

1. **Fake Coupons:** Scammers distribute fake coupons promising steep discounts. These coupons are often shared via e-mail, social media and fake websites designed to mimic legitimate retailers. Remember: if it feels too good to be true, it probably is.

⚠ **How to avoid:** Always verify a coupon by checking the retailer's official website or app, and avoid clicking on links in unsolicited e-mails.

2. **Phony Websites:** To steal personal information, fake websites mimic legitimate online stores using similar logos, branding and URLs that are only slightly different from the official sites.

⚠ **How to avoid:** Check for secure website indicators such as HTTPS and a padlock icon in the address bar. Read reviews and quickly search the website's legitimacy before making any purchases. Pay attention to the URL for any unusual characters or misspellings.

3. **Fake Delivery And Nondelivery Scams:** Scammers send fake delivery notifications or claim a package is undeliverable to trick you into providing personal information.

⚠ **How to avoid:** Track orders directly through the retailer's website or app. Avoid clicking on links in suspicious messages, and be cautious of unsolicited delivery notifications.

4. **Fake "Order Issue" Scams:** E-mails claiming a problem with your order and asking for personal details are common. These messages often look like they come from well-known retailers.

⚠ **How to avoid:** Contact customer service directly through the retailer's official channels to verify any issues, and avoid providing personal details through links in unsolicited messages.

5. **Account Verification Scams:** Scammers send e-mails or texts asking you to verify your account information. These messages often include links to fake login pages.

⚠ **How to avoid:** Never provide personal details through links in unsolicited messages; instead, log in directly to your account through the official website.

6. **Gift Card Scams:** Scammers offer discounted gift cards or request payment via gift cards. Once the card numbers are provided, the scammer uses the balance, leaving the victim with a worthless card.

⚠ **How to avoid:** Purchase gift cards directly from reputable retailers and never use them as a form of payment to unknown individuals.

Avoid Scams And Create A Safer Shopping Experience

Nothing will kill the holiday shopping spirit like $1,000 worth of fraudulent charges on your credit card or gifts from phony sites that never arrive. Cybercriminals take advantage of the festive shopping rush, and consumers' tendency to take more risks during this time only amplifies the danger. By verifying sources, checking website security and avoiding unsolicited links, you can enjoy a safer shopping experience this season!

"I DIDN'T KNOW"

Unfortunately, That Excuse Doesn't Replenish Your Bank Account, Resolve A Data Breach Or Erase Any Fines And Lawsuits.

It's coming...

- That day a hacker steals critical data, rendering your office useless...
- That day when your bank account or credit card is compromised...
- That day when your customers' private lives are uprooted...

Cybercriminals and hackers are constantly inventing NEW ways to infiltrate your company, steal your assets and disrupt your life. The ONLY way to STOP THEM is this:

You Must Constantly Educate Yourself On How To Protect What's Yours!

Now, for a limited time, we have the perfect way to help reduce your risk and keep you safe! Simply sign up to receive our **FREE "Cyber Security Tip of the Week."** We'll send these byte-sized quick-read tips to your e-mail inbox. Every tip is packed with a unique and up-to-date real-world solution that keeps you one step ahead of the bad guys. And because so few people know about these security secrets, every week you'll learn something new!

Get your FREE "Cyber Security Tip of the Week" at:
https://www.adrem.com/cyber-security-tip-of-the-week/

SAFE CYBER PUZZLE

CYBERSECURITY AWARENESS MONTH

SECURE OUR WORLD

Double Puzzle

Solve the anagrams and use the circled letters in the top part to complete the final phrase at the bottom. Each circled letter is used just once.

AOSDRPWS

TNRETENI

UTDPEA

YRISTCEU

PYRICAV

PECTOMUR

AEKCHR

EEICVD

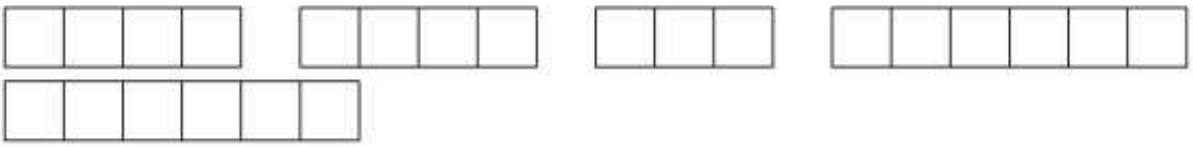
IWIF

RCEBY

IRYFEV

ELARMWA

GOILN



CYBERSECURITY AWARENESS MONTH

Look for answers in Next Month's issue or download at: https://www.adrem.com/puzzle/

CARTOON OF THE MONTH

"It's one of those new Instant Cauldrons. You put a kid in here with some eye of newt and an hour later it's the best thing you've ever eaten."

HAUNTED SMARTWATCHES

It's Halloween, and Apple Watch users are getting a bit of a scare. "Ghostly" taps, swipes and calls are happening on smartwatches without physical touch. It's either their late great-granny trying to say hello from the afterlife, or...it's a glitch. Apple is leaning toward the latter. *MacRumors* shared an internal memo stating, "Some customers may report their Apple Watch Series 9 or Apple Watch Ultra 2 is experiencing false touches on their display." Sometimes, these phantom activities prevent users from entering their passcode. If you experience "ghost" glitches on your smartwatch, Apple recommends restarting your device and keeping your software up-to-date.

FROM HERO TO ZERO TO HUMAN:

LANCE ARMSTRONG'S ADVICE FOR BOUNCING BACK FROM BIG MISTAKES

Former professional cyclist Lance Armstrong was widely celebrated for his seven consecutive Tour de France victories from 1999 to 2005. A cancer survivor and elite athlete, he was a hero to many. However, in the early and mid-2000s, his career was marred by a highly publicized doping scandal. The United States Anti-Doping Agency stripped Armstrong of his titles and banned him from professional cycling for life after concluding he had used performance-enhancing drugs throughout his career.

Armstrong's public mistake cost him over $100 million, his career, his reputation and many friends. But he chose not to curl up in the fetal position and lose what he still had left: his wellness, lifestyle and family. He embraced his mistake, eventually rebuilding his professional and personal life. Today, Armstrong is an entrepreneur, philanthropist, podcaster, author and speaker who is open about what it took to go from hero to zero to human. At a recent industry conference, Armstrong spoke to entrepreneurs about how he survived his downfall and rebuilt a career and life he's proud of.

Choose An Authentic Path Forward

After being banned from professional cycling, losing endorsements and many personal relationships, Armstrong felt he had three choices: lie down and give in to the suffering, retain some of his endorsements by becoming the face of anti-doping campaigns or try to rebuild on his own. He chose the latter. "Anti-doping wasn't my life's work, and it never will be, so I chose a more renegade path," he explains. "It took longer, but I walk my path every day, I'm glad I chose the path I did."

Armstrong focused on his passion for investing, including early-stage investments in companies like Uber and DocuSign, which eventually paid off in spades.

Authenticity in his personal life was essential, too. "We all live these interesting lives, and it's just a big canvas. At the end of the day, we get to look at the painting and say, 'What do you think? How are you, Lance, as a friend? How are you as a father? How are you as a husband?'" he says. Working on being a good father, partner and friend kept him focused on his path forward.

Maintain Wellness

Despite the upheaval, Armstrong maintained important routines like cycling and swimming, and maintained the rhythm of staying healthy and focused. Still, the experience was traumatic. "I had to do a lot of work to remedy that," he explains. "I'm talking deep work, trying to understand early life, early career, the downfall, where we go from here…. I've devoted a ton of time on that."

Lean On Your People

After he had admitted his mistake, Armstrong lost half his friends and working relationships. Still, close friends and family remained. "As much as that sucks, you see these folks who are like, 'I'm here right now. Now we go. Now we rebuild,'" Armstrong recalls. "I think that's the most important thing: if there are ever any headwinds working against you, that team of folks around you has to be the right team. People are everything."

SHERPA COMPLIANCE CONSULTING

Specialized Guidance for Navigating Government Regulations

Is your business facing compliance challenges with standards like HIPAA, NIST, CMMC, or FTC? Our team of specialists is here to help you build or improve your compliance program, ensuring your organization meets all necessary requirements.

Our Services Include:

- **Compliance Program Development:** Start from scratch or refine your existing program with specialized support.
- **Vulnerability Scanning & Penetration Testing:** Identify and address potential security gaps.
- **Trusted Partnerships:** We work closely with auditor and certification organizations, as well as recommended IT providers, to deliver a comprehensive approach to your compliance needs.

SHERPA An AdRem Company

Get Started With Our Free Resource!

Download our guide, *6 Essential Elements of an Effective Compliance Program*, for a practical introduction to starting your compliance journey.

Visit: https://thesherpa.us/6-essential-elements/
or
Call Our Office at (571) 360-3926.

TRIVIA

No longer just an anti-alien tool, what product did rapper M.I.A. launch in her new company, Ohmni?

A. Pocket-Size Laser
B. Magnetic Tent
C. Tin Foil Hat
D. Bluetooth Sound Wave Generator

OUR SERVICES

IT BUSINESS SOLUTIONS

Managed and Co-Managed Service (MSP)
Managed Security Service (MSSP)
Cloud Computing
VoIP Solutions
Data Backup and Recovery
Cybersecurity
Vendor Management
Hardware as a Service (HaaS)
Secure Access Service Edge (SASE)
Virtualization
Remote Work Environments

COMPLIANCE SOLUTIONS

CMMC, NIST, HIPAA, ISO, FTC, etc.
Email Enclaves
Employee Security Training
Data Backup and Recovery
Data Privacy and Encryption
Disaster Recovery Planning
Penetration Testing
Vulnerability Scanning
Policy Consulting
Cybersecurity Consulting

HARDWARE PROCUREMENT

Shop.AdRem.com

HOSTING & ONLINE SERVICES

OnlineServices.AdRem.com

Domain Registration and Transfer
Website Hosting: Website Builder & WordPress
Website Security Solutions
Custom Website Design
WordPress Website Support Solutions
Logo Design
Virtual Private Servers (VPS)
Dedicated Servers
Email Marketing

LIGHTS OUT FOR BUSINESS:

Resiliency Amid Internet Outages

OUR MISSION

To apply our 20 Year Legacy of knowledge and innovation, to defend Critical IT Networks, and encourage a more secure nation of Tomorrow by delivering Today's technologies with respected, trusted, and proven individuals.

THE PUMPKIN PLAN

By Mike Michalowicz

The Pumpkin Plan, by Mike Michalowicz, is a must-read for small-business leaders wanting to carve out a niche and grow their business effectively, especially during the bustling holiday season. Michalowicz presents a straightforward, actionable strategy to cultivate a remarkable business by focusing on top clients and eliminating unprofitable ones. The book is filled with practical advice and real-world examples, making complex business concepts easy to understand and implement. His engaging storytelling and clear, step-by-step approach provide a refreshing take on business growth. This book is a valuable resource for any small-business owner looking to streamline operations, maximize profits and achieve sustainable success.

Businesses are increasingly reliant on the Internet. CRM platforms, virtual meeting apps, online sales, POS systems and even office printers require the Internet so you can do everything you need to deliver high-quality products and services to your customers. However, Catchpoint's 2024 Internet Resilience Report states that 43% of businesses estimated they lost "more than $1 million due to Internet outages or degradations in the month prior to the survey."

It's tempting to blame the Internet provider when the Internet goes out. Unfortunately, outages happen. Pointing fingers at vendors won't change that. Instead, the solution must come from within.

What's Going On With Internet Connectivity

In July, a global Internet outage forced millions of computers offline, including at major airlines, banks and hospitals. The root cause of the disruption was a single software update deployed by cyber security firm CrowdStrike.

Cyber security reporter Brian Krebs famously described the Internet as "held together with spit and baling wire." It's easy to forget that the Internet, like other tech, is evolving and complex. It connects countless systems and devices globally, creating a web of dependencies. A disruption in one part of the network can ripple through and affect other systems, as seen with the CrowdStrike update. Internet outages can have serious financial and security consequences, so preparing for an outage is crucial.

Resilience Comes From Within

After an outage, you may be tempted to fire your services provider. However, Catchpoint CEO and co-founder Mehdi Daoudi explained in an interview with Tech Brew that it's not a good solution (unless they prove unreliable). Daoudi said that after an outage, it's better to work with your vendors to figure out what went wrong and how to be better prepared. Some companies have hired chief resilience officers, but the title doesn't matter as much as having a leader in your company who spends time thinking about resiliency.

"It's important that companies embrace resiliency and reliability. How? By encouraging the learning from failures, by not firing," Daoudi told Tech Brew. "What did we learn from this outage? What can we do to strengthen our postures going forward?"

The Internet is complex, and outages happen. To safeguard against the inevitable, businesses must cultivate resilience internally and proactively collaborate with Internet vendors to avoid damaging consequences.