The tech chronicle

Sirtawn Systems

Start Fighting Cyber Crime with Knowledge and Action.

Our Newsletter for Issue #176 is dedicated to Cybersecurity Month

Keep your data safe!
It will affect your Business.

WHAT DO YOU DO WHEN A COMPANY COMPRISES YOUR DATA?

1. Your data may be leaked – How do you respond?
2. Is your data backed up offsite in a safe location?
3. Is your network isolated from the internet?
4. Do you have a strong security policy for employees (Network & Data Security)?
5. Do you have specific "Password" guide lines and "Usage" Policies?
6. Do you have specific employee "Internet Usage" guide lines for security?

Key Elements of a complete Data Security Policy.

(Reprinted from a previous newsletter – most important!!!!)

- Safeguard Data Privacy.
- Password Management.
- Internet Usage.
- Email Usage.
- Company Devices.

***Safeguard:** Apart from complying with the existing rules & regulations, a privacy policy will guide your employees on how to handle sensitive information in such a way that is not compromised.

***Passwords:** Setting up a password policy will ensure your company Resources are protected and only accessible by authorized personnel. The guidelines should include password length, complexity and how often it needs to be changed

***Internet:** An internet usage policy that defines best practices while accessing the internet, such as restricting employees from visiting certain sites or prohibiting unnecessary file downloads, will help set limitations and minimize security risks.

***Email Usage:** Companies often fall victim to data breaches due to employee negligence or email misuse. With an email policy in place, your employees will be aware of what is expected of them and how company information should be disseminated internally.

***Company Devices:** As the use mobile devices for work gains momentum, it also opens the door to several security threats. Implementing a comprehensive policy will help mitigate the risks associated with data theft and stolen devices.

Key Elements of a complete Data Security Policy

Personal Employee Devices.

Social Media Presence.

Software User Agreements.

Reporting Security Breaches.

Employee Devices. Unlike company-owned devices its difficult to have complete control over personal devices. A security policy, such as accessing company resources only through a secure VPN or installing an antivirus or mobile device management software will set certain boundaries or limitations.

Social Media. Protecting your company's reputation is critical not only within the workplace but outside as well. A social media policy will help you regulate your employees' online actives.

Software Agreements. Violating a software license agreement can lead to legal implications. A software user agreement policy will ensure your employees comply with the procedures regarding the appropriate use of company-owned software.

Reporting Security Breaches. Implementing a Security Incident Reporting policy is important to minimize negative impacts. Your employees should be educated on how to report real or suspected security breaches and what steps they need to take to prevent the from happening.

Data Security Risks can arise at any time and from anywhere!

Your Network + Data Security is the Backbone of your business. All elements must be protected to completely protect your business and your future.

6 Shopping Scams and How to Avoid Them!

Now it's November, October was Cyber Security Month. Have you installed any of the above suggestions to protect your company? Also, November means the biggest online shopping day of the YEAR is just weeks away: Cyber Monday (December 2, 2024). Unfortunately, it's also open season for cybercriminals. 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 North America in 2023. Also, 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.

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 Non delivery 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!

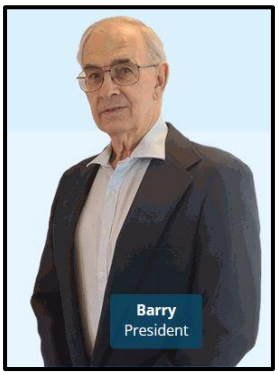
Now, for a limited time, we have the perfect way to help reduce your risk and keep you safe! Simply sign up to receive our **FREE "Cyber Security Tip of the Week."** We'll send these byte-sized quick-read tips to your e-mail inbox. Every tip is packed with a unique and up-to-date real-world solution 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: Sirtawn.com

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."

Our Assessment Offer



This monthly publication provided courtesy of Barry Brown, President of Sirtawn Systems.

FIGHTING CYBERCRIMINALS ON YOUR OWN CAN BE TIRING WHEN YOU HAVE A BUSINESS TO RUN.

CONTACT US TODAY

FIND OUT WHAT IT'S LIKE TO HAVE OUR CYBERSECURITY EXPERTS IN YOUR CORNER.

We are offering a FREE Network Security Audit with no obligation. You will receive a "Cyber Security Audit" outlining our findings following the audit. Again … **NO Obligation….**

Sirtawn Systems

Your Cyber Security Experts

Phone: (905) 947-1636
Website: www.sirtawn.com
Email: sirtawnsystems@gmail.com