SYSTEL®

800.849.5900 | www.systeloa.com

Managed IT

Cybersecurity Awareness

Cyber threats are evolving – are you keeping up? From QR code scams to the critical importance of two-factor authentication, this blog breaks down the top cybersecurity risks you need to know about- and how to protect yourself. Whether you're a business owner or just want to stay safe online, these insights will help you take control of your digital security.

CYBERSECURITY AWARENESS

In today's interconnected world, the importance of cybersecurity cannot be overstated. As we rely more heavily on digital platforms for both personal and professional activities, the risks associated with cyber threats have grown exponentially. Here, we aim to shed light on various cybersecurity topics, from emerging threats like quishing to essential practices such as enabling two-factor authentication (2FA) and regularly updating software. By understanding these issues and implementing effective strategies, you can better protect your sensitive information and maintain your digital safety.

1. Quishing

You may know about phishing, but have you heard of "quishing"? Quishing is a hacking technique where scammers use fake QR codes to lead you to harmful sites or downloads. This can happen not only in emails but also in physical form such as printed signs, flyers, or stickers. Some scammers have even placed stickers ON TOP OF legitimate QR codes such as the ones used for restaurant menus.

Here's how to stay safe:

- **Verify Links:** Treat QR codes like you would email links—check before you click
- **Physical QR Codes:** Instead of scanning QR codes on menus, flyers, etc, go directly to the restaurant or company's website for menus and other information

- **Double-Check Email Senders:** Confirm the sender's identity over the phone and look out for exact spelling of names and email addresses.
- **Be Careful on Mobile:** Mobile devices often hide full email addresses, so delay actions until you can review on a computer.

2. Two-Factor Authentication (2FA)

In today's digital age, protecting your personal information is more important than ever. Two-factor authentication (2FA) is an easy way to add an extra layer of security to your accounts. By requiring not just your password, but also something you have—like your phone or a security key—2FA makes it significantly harder for cybercriminals to gain unauthorized access. Even if they somehow manage to steal your password, they still can't get in without that second factor. It's a simple step you can take to prevent identity theft, fraud, and data breaches.

Where should you enable 2FA? Anywhere you store sensitive information or value your privacy. Start with your email accounts, social media profiles, and online banking. These are often prime targets for hackers. Many major services like Google, Facebook, Instagram, and your financial institutions offer 2FA, and enabling it could be the difference between keeping your data safe or losing control of your accounts.

3. Update Your Software

Building on our recent discussion about quishing (QR code phishing) and the importance of 2FA, let's reinforce a few essential cybersecurity practices. Always exercise caution when clicking links or downloading attachments, even if the email appears legitimate—phishing attacks often mimic trusted sources. Be wary of emails that seem urgent, like those claiming someone tampered with your account and asking you to call a number to verify your information. These could be phishing attempts designed to steal the very information they claim to protect. Instead, verify such requests through official channels, like the company's website or a phone number you trust.

Keep all software updated, including your mobile phone software, as updates often contain critical security patches. If your phone is no longer receiving security updates, it's time to upgrade to ensure your data remains protected. Using strong, unique passwords across different accounts and staying alert to anything suspicious are vital habits. Remember to report any unusual activity right away—early detection can prevent small problems from becoming big ones. Cybersecurity is a shared responsibility, and together we can help keep our systems safe!

4. Protect Your Data!

In today's digital world, data loss can happen at any time, whether due to ransomware attacks, hardware failures, or accidental deletions. That's why regular backups are crucial for ensuring that your important files are safe and recoverable.

Why You Should Back Up Your Data:

Backing up your data is one of the most important steps you can take to protect yourself from unexpected loss. In the event of a ransomware attack, having a secure backup can save you from having to pay a ransom to recover your files. Regular backups also provide peace of mind against accidental deletions—because mistakes happen—and ensure you can quickly restore any lost data. Additionally, since hardware can fail without warning, keeping backups helps minimize the disruption and damage caused by system failures.

Best Practices for Backing Up Your Data:

- **Follow the 3-2-1 Rule:** Keep three copies of your data (one primary and two backups), store the copies on two different types of media, and keep one backup offsite.
- **Automate Your Backups:** Use software that automatically backs up your data at regular intervals, so you don't have to remember to do it manually.
- **Test Your Backups:** Regularly check that your backups are working and that you can successfully restore files from them.

5. Social Engineering Attacks

Many cyberattacks exploit human psychology rather than complex hacking. Social engineering tricks people into revealing sensitive information or access. Attackers may impersonate trusted contacts, send fake alerts, or create urgency to deceive you into clicking links, sharing data, or wiring money.

How to Stay Safe:

- **Verify**: If something seems off, contact the person or organization directly using known contact details.
- **Take Your Time:** Don't let urgency pressure you; think critically.
- **Limit Sharing:** Don't share sensitive info if you didn't initiate contact.

Cybersecurity is a continuous journey that demands vigilance, awareness, and proactive measures. Whether it's guarding against sophisticated phishing techniques like quishing, enhancing account security through 2FA, or ensuring your data is backed up and software is up to date, each step you take contributes to a safer digital environment. Remember, the key to effective cybersecurity lies in staying informed and being prepared to respond to potential threats. By adopting these best practices, you can safeguard your digital life and navigate the online world with greater confidence and peace of mind.

To learn more, Contact Us today!