It's time to check your security as tax season comes around

Computer security is an unfortunate fact of modern payroll administration—especially right now, when phishers and scammers know you and your staff are busy and distracted. You already know to not respond to email requests from so-called executives who need employees' W-2 data emailed to them ASAP. This scam seems quaint by today's standards. New scams, intent on separating employees' personal identifying information from your server, surface with regularity. You might find what's new quite alarming.

New malware steals saved passwords

Good computer hygiene says you shouldn't use the same password for multiple websites. So web browsers first suggest a strong password of random letters, numbers, and symbols and then ask whether you'd like it to remember your password. Don't click Yes.

New malware, called Redline Stealer, can grab passwords, even from VPNs. We suggest the old-fashioned way of storing passwords: Write it down on paper and lock the paper in your desk.

First phishing, now QRishing

If you're thinking of using QR codes—those square barcodes that smartphone cameras scan and read to provide quick access to a website—to ramp up security on the website to which you post employees' W-2s, you might want to think again.

The FBI's Internet Crime Complaint Center reports cybercriminals are tampering with QR codes to redirect victims to malicious websites engineered to steal login and financial information. Malicious QR codes may also contain embedded malware, allowing criminals to gain access to employees' mobile devices to steal their personal information.

IC3 offers tips you can pass along to employees:

- Once you scan a QR code, check the URL to ensure it's the site you intended to go to and looks authentic. A malicious domain name may be similar to the intended site but with typos or a misplaced letter.
- Practice caution when entering login, personal or financial information from a site navigated to via a QR code.
- Don't download apps from QR codes; use your phone's app store for safer downloads. Likewise, don't download a QR code scanner app. *Why:* This increases your risk of downloading malware onto your device. Most phones have built-in scanners through the camera app.
- If you receive a QR code you believe is from someone you know, reach out to them through a known number or address to verify the code is from them.

7600 Leesburg Pike, Suite 300, Falls Church, VA 22043-2004 (800) 543-2002

Your W-2 data or else....

Ransoming your company's data is apparently easy to do**.** According to the National Institute of Standards and Technology (a branch of the Commerce Department), all it takes is four steps for a cyberthief to access your data for ransom:

1. You're tricked into clicking on a malicious link, which downloads a file from an external website.
2. You execute the file, not knowing the file is ransomware.
3. The ransomware takes advantage of vulnerabilities in your computer and other computers to replicate itself throughout the company's computers.
4. The ransomware simultaneously encrypts files on all computers, then displays messages on screens demanding payment in exchange for decrypting the files.

Thankfully, the steps needed to protect against ransomware are basically the same steps you need to take to protect your computer systems in general:

- Use antivirus software and make sure it automatically scans emails and flash drives for ransomware and other malware.
- Keep computers fully patched.
- Use security products or services that block access to known ransomware sites.
- Configure operating systems or use third-party software to allow only authorized apps to run on computers; this prevents ransomware from working.
- Restrict or prohibit the use of personally owned devices on the company's network. Take extra steps to assure security for employees who work from home (e.g., ensuring employees don't allow family members to use their work computers).

NIST and CISA (Cybersecurity and Infrastructure Security Agency) have tons of tips you can use and pass along to your employees. Point your browser here, here and here for more information.

7600 Leesburg Pike, Suite 300, Falls Church, VA 22043-2004 (800) 543-2002