Make Cyber Security Awareness a Focus for 2023

Consider the following statistics. Cybercrime increased 600 percent during the pandemic, and 95 percent of cyber incidents occur due to human error. Cyber threats have grown in number and sophistication, and thus cyber security awareness must also move to the next level. Forward thinking organizations will make this a priority for 2023.

During cyber security awareness month, the Cybersecurity and Infrastructure Security Agency (CISA) emphasized four key habits to encourage in your staff:

- Think before you click (recognize and report phishing)
- Keep software up to date
- Use strong passwords
- Enable multi-factor authentication (MFA)

Recognize and Report Phishing

For years, cyber criminals have used phishing to capture sensitive information or gain unauthorized access. Phishing, a common form of social engineering, involves a bad actor sending a seemingly trustworthy email. The email might prompt the victim to reply with sensitive information. Or it might include a link to a phony website or malicious file.

To protect against phishing attacks, organizations can and should use anti-virus and anti-malware programs, firewalls, and email filters. However, even with the best technology, phishing attacks will happen. Thus, the best defense lies in empowering cyber aware employees who recognize, report, and respond appropriately to phishing attempts.

Train every employee to recognize the signs of phishing. These can include a generic greeting or subject, spelling or grammar errors, a sense of urgency and unusual requests for confidential information or money. Employees should also know how to spot potentially fake email or website addresses. And they should know how to report suspicious activity.

To cement security awareness training, bring it home with phishing simulations. In a simulation, users periodically receive emails that mimic a phishing email but do not pose any real danger. Administrators track the emails and responses to determine the effectiveness of training and provide any necessary follow up.

Apply Software Updates Promptly

Any given computer, laptop or mobile device contains dozens, even hundreds, of software programs. These include not only the productivity apps like word processing but also device drivers, audio players, anti-virus programs, operating systems, and web browsers.

Periodically, software vendors will release updates to their programs. And all too often users and companies delay installing these updates. This introduces a significant security risk, as one common purpose for updates includes patching security vulnerabilities. Hackers keep an eye on vulnerability reports, and they will exploit them.

Organizations should take time to implement a patch management program. This will involve taking an inventory of all assets and security systems and creating a timeline and process for installing patches on a regular basis.

Manage Passwords and PINs

Over 60 percent of data breaches involve stolen or weak credentials (username and password). For instance, if hackers can gain the credentials for a highly privileged user, they can steal data or create havoc in the system. Consequently, companies need to create and enforce strong password policies.

As a rule, passwords should not include actual words, nor should they include numbers in a sequence. Create a long password with a combination of upper-case and lower-case letters, numbers, and symbols. To make things easier and safer, consider using a password manager with a built-in random password generator.

IT departments and other users with high-level access need to be particularly careful. Be sure to change default passwords. And never share or reuse passwords.

Enable MFA

Passwords alone will not provide sufficient protection. However, statistics from both Microsoft and Google show that using MFA as an additional security layer can thwart nearly 100 percent of automated attacks.

When implementing MFA, implement across the entire organization to avoid leaving doors open for hackers. And, because the success of an MFA program depends on user experience, make usability a priority. Educate end users and give them choices of what authentication factors to use, whether biometrics, an authentication app, or some other factor.

Make Cyber Security Awareness Integral to Company Culture

To prove effective, cyber security awareness requires a deliberate, multi-faceted approach. When consistently and properly educated about security threats and security best practices, your users can become your best defense.

eMazzanti stands ready to help, with educational materials, free security assessments and a full menu of cyber security tools and services.