THE MONDAY 03/09/2018
MS. STAR 2

Good time to beef up cybersecurity

As more companies come under attack from hackers, it's more crucial than ever to make sure everyone in an organisation is sensitive to the need for computer security.

By JOYCE M. ROSENBERG

COMING back to work after a long break? It's as good a time as any to make sure you and your staff are on the same page when it comes to cybersecurity.

Here are some basics that owners should emphasise to their staffers:

Passwords

Start with creating a strong password. It's probably a good idea for the company to have minimum requirements for passwords used to access its systems. Those requirements should include a mix of upper- and lowercase letters, numbers and symbols.

Many businesses are using two-factor authentication, which requires people to enter a code in addition to the login/password combination. They may also require staffers to periodically change their passwords.

Phishing alerts

Bosses should remind everyone to be vigilant about phishing scams, which can plant malicious software on a computer or phone. Everyone should understand that they shouldn't click on any link or attachment in an email unless they're sure it's legitimate. It should be standard operating procedure to check a sender's email address to be sure it's correct and not suspicious, and the body of an email should be checked for any oddities that can be hallmarks of phishing scams.

As new staffers are trained, they should learn about the kinds of emails they can expect to receive. The more familiar they are with a company's customers, vendors and other contacts, the better they'll be at spotting suspicious emails.

Locking phones and laptops

Staffers who can access the company's systems including its email via smartphones and laptops – whether they're personal or company-provided – should be required to lock their devices with codes or passwords.

Downloading updates

If the company has an information technology staffer or department, it should be aware of security and other updates issued by Microsoft and other companies. Each company device should be updated. If there isn't a dedicated IT staffer, the owner or another manager needs to be sure that all updates are downloaded.

The owner's responsibility

A survey issued earlier this year by insurer Hiscox found that only half of small businesses said they had a clear cybersecurity strategy. Making systems as secure as possible often gets put on the back burner while an owner works with customers and staffers.

Companies without IT staffers should consider bringing in a consultant who can assess what's needed to increase security. Among the items companies need are anti-virus and anti-malware software, firewalls, encryption software and offsite storage that continually creates new versions of all of a company's data.

Those versions will be critical if a company's computers are victims of ransomware attacks that render files and documents unusable. – AP

Businesses should have a clear cybersecurity strategy and bosses must remind their staff members to be vigilant at all times. — 123rf.com