The General Ledger
The Complete Newsletter For Professional Bookkeepers

OCTOBER, 2016 VOL. 33, NO. 10

Getting Hacked

Do not assume hackers will ignore you because you're small. A report by Keeper Security and the Ponemon Institute reveals that roughly half of all small businesses have been hacked within the last year, possibly due to poorer security than large corporations, but also to being less careful with the security they have.

The first step to improved security is to know what the most common forms of cyber attacks are:
∗ Advanced persistent threats (APTs). Long-term hacks that compromise a targeted system in phases.
∗ Distributed denial of service (DDoS). A server is swamped with so many requests that the targeted system or website is shut.
∗ Inside attack. Someone with administrative privileges, usually a current or former employee, has access to confidential data. Employees who leave should immediately have their system access revoked.
∗ Malware ("malicious software"). Any program introduced into your system to cause damage or gain unauthorized access.
∗ Password attacks. Hackers guess until they hit the right PW (brute force attack). They use a program that tries different combinations of dictionary words (dictionary attack); or they track all of the user's keystrokes, including PWs (keylogging).
∗ Phishing. Getting sensitive data such as logins and credit card info by enticing you to go to websites that seem legitimate but are not.

The next step is to add security to your system, such as:
∗ Antivirus software. Defends against most types of malware.
∗ Firewalls. Help prevent unauthorized users from accessing computers or networks.
∗ Data backup solutions. Recover lost data that has been stored at another location.
∗ Encryption software. Protects sensitive data by encrypting it.
∗ Two-step authentication software. Reduces the possibility of a password being cracked by requiring two unique pieces of information for log-in.
∗ Cybersecurity Insurance. Helps recoup losses and expenses associated with a data breach. Make sure the policy includes first- and third-party coverage, to cover first-party costs such as business interruption, legal fees, public relations, etc.; and third-party costs such as lawsuits for exposure of customers', vendors' or other outsiders' sensitive data.

Lastly, best business practices may seem unimportant, but they matter:
∗ Keep your most-used software up to date.
∗ Educate employees on how to recognize a data breach as well as best practices to avoid one.
∗ Put formal security policies in place; the most important one is strong passwords.

Source: Sammi Caramela,
"Cybersecurity: A Small Business Guide,"
www.businessdaily.com
July 11, 2016