

HACKER-PROOF SECURITY PRACTICES

> Check out this list of well-known companies: Target, Neiman Marcus, Michaels, Home Depot, AT&T, P.F. Chang's, UPS, J.P. Morgan and Dairy Queen. They were all hacked in 2014. Customer data, mostly credit card information, was stolen.

Intimidated by the horror stories of these major companies? Don't be. Small-business owners can protect themselves and their customers by employing simple yet very effective security practices with low-cost, easily applied solutions.

Pack Some Password Power

Strong passwords are your first line of defense. It's good practice to change them monthly.

For example, here's a strong password I used last year: *[365m4yb3r-ryl1n3r0ad](3)]*. I know what you're thinking: Huh? But when you examine the password closer, the "formula" makes perfect sense.

I once lived at 365 Mayberry Line Road. In the password, I changed the vowels into numbers that look like them: A = 4, E = 3, I = 1, O = 0. Next, you'll see the number 3 in parentheses (3); this represents the month of March. When I updated the password in April, that number changed to 4. Lastly, I surrounded the whole thing with "[]*" because the strongest passwords use numbers, letters and symbols.

With these simple techniques, you can develop passwords that only you remember and change. You can adjust the symbols based on the requirements of websites, to accommodate symbols that aren't allowed or to incorporate required formatting options, such as capital letters.

Another solution is using a free program such as LastPass (lastpass.com). Download the program to install a button on your browser, and then submit a strong password. As you enter secure websites, LastPass will begin saving passwords securely for future use.

Invest \$12 a year and you can extend LastPass coverage to mobile devices.

Speaking of browsing, most of the malware you get on websites targets those using Internet Explorer as their browser. Consider using free alternative browsers such as Google Chrome (google.com/chrome) or Mozilla Firefox (mozilla.org).

Update the Operating System

April 8, 2014, is an important date in computing history. That's when Microsoft stopped supporting the XP operating system. So if you're still on XP, upgrade now to at least Windows 7 Professional or 8.1 Pro. If you don't, you



are no longer PCI compliant (check with your POS vendor) and are at high risk of getting malware. You can get a license for an upgraded OS for about \$140 at newegg.com or microcenter.com. Get the "OEM" version.

Once you have an updated OS, it's up to you to maintain it. Go to Start (Windows logo in lower left) > Control Panel > System and Security > Windows Update > Change Settings. Set this to "Install updates automatically" and check all the boxes below this selection.

For Macs, the latest OS is Mac iOS 10.10.3. To set up automatic updates, go to the Apple symbol (upper left) > System Preferences > App Store. Then check all the boxes on this screen. Hit "Check Now" while you're there to grab the latest updates.

Stop Viruses and Malware

The next layer of protection involves anti-virus and malware software installation.

For PCs, check out the free programs Avira (avira.com/en/avira-free-antivirus) or Avast (avast.com). If you're using Windows 7, you can also download Microsoft Security Essentials (microsoft.com/security/portal/mmpc). (Windows Defender is included in Windows 8.1 and is activated when you turn on your PC.)

Although Macs are harder targets for hackers, it's still good practice to install protection. Use either Avast (avast.com/free-mac-security) or ClamXav (clamxav.com).

Embrace Two-Factor Authentication

Beyond passwords and protective software, two-factor authentication is the best security practice. As the name implies, to access your account, you'll need a password and a numerical code, which changes constantly.

This code is either sent by text to your smartphone or generated by an app; the only way someone gets in is if she or he has both your password and your smartphone.

Start by downloading the App Authenticator for Apple iOS or Google Authenticator for Android. Many services (Google, Dropbox, Microsoft, etc.) use these apps to generate the numerical code. You may have to dig deep into your login-required websites to enable this feature, but it's well worth the peace of mind it delivers. 🌿

Renato Sogueco is SAF's chief information officer and the industry's go-to tech guy. rsogueco@safnow.org