TECH BRIEF

The perils of passwords and how to avoid them

ENJOY SAFER TECHNOLOGY™

THE PERILS OF PASSWORDS AND HOW TO AVOID THEM

By Graham Cluley, We Live Security

Sometimes it feels monumentally difficult to convince Internet users to get smarter about their passwords. One of the biggest problems is password reuse. Most people use the same password for multiple websites. In some cases, users will use the same password for every website they access. This leads to big problems. Because if you use the same password at websites X, Y, and Z, a hacker who steals your password from website X can use it to break into your Y and Z accounts. Maybe X, Y, and Z have done their homework, realized that it's important to build a secure, hardened website, and kept up to date with their software patches. Maybe they have great security in place, and hacking attempts will end in failure.

Well, there's still a problem. And that's the user's computer. If your computer has been infected by keylogging malware, then a criminal hacker can easily capture your password and try it out on other sites. Indeed, many banking Trojans do precisely this—effectively looking over your shoulder every time you enter a password into an online form and grabbing it for later exploitation. Maybe you are running a top antivirus product on your computer, are diligent about keeping your security in place, and are careful about what programs you install, and your software updates are always nice 'n' fresh.

Good for you. But there are still problems.Because what's to stop you being phished? Are you smart enough to tell the genuine emails from the bogus ones? Are you sure? The staff at Forbes, CNN, The Washington Post, and countless others certainly weren't. They all got tricked by the Syrian Electronic Army, which forged emails to look like they were genuine, but with links that took staff to phony phishing websites designed to steal login details and allow the hackers to deface websites and publish pro-Assad messages on Twitter. However, it's possible that you are on the lookout for phishing emails, and have learned to be dubious of unsolicited messages or websites that ask unexpectedly for your login credentials to be re-entered.

But, as the last few days have proven, there's still a problem. What if your computer isn't compromised by malware, and you aren't visiting a phishing website, and the website is set up properly using SSL to protect your communications, and yet you can still have your private information intercepted by hackers because your operating system has a bug in it? Right now that's the case with iPhones and iPads (if you haven't installed the iOS 7.0.6 update yet), and users running Mac OS X Maverick (which doesn't yet have an official patch from Apple).

A critical security flaw in iOS and Mac OS X allows hackers to intercept what should have been secure communications between your Apple computing devices and the outside world. When serious bugs like this existing in the operating system, it makes life too easy for online criminals to act as the man in the middle, stealing what should have been secret information in transit. While the world is waiting for an OS X fix from Apple (and updating its iPhones and iPads), what lessons can we learn from all of these problems?

Well, one message you should be hearing loud and clear by now is that passwords come with problems. Passwords can be stolen—by phishing, by malware, by hacking, via vulnerabilities. For those online accounts that you really want to keep secured, a stronger form of protection is required. One obvious solution is two-factor authentication (2FA), which requires a unique one-time password for every login attempt. Even if your regular password is guessed, cracked, or stolen by hackers, it won't be any use to the bad guys

because they won't know what your one-time password is. Indeed, if you use something like a mobile phone app to automatically generate your one-time password, then it's always likely to be within easy reach for you, but far away from the clutches of the hackers. When a website or service offers you the option of two-factor authentication, please consider enabling the feature.

And if you run an online service or provide systems so your staff can access company information remotely, why not consider offering two-factor authentication to reduce the risks?

Sites like Facebook, Google, Twitter, Dropbox, and others do provide two-factor authentication to better secure accounts, but far too many still offer nothing for those who want a higher level of protection.

2FA may not be the magic bullet that kills all online criminal activity in its tracks, but it certainly makes life an awful lot harder for the hackers who want to break into your accounts.