News & Opinion

Why Facebook 'Sucks': A Lesson in Online Security

cont. from page 1

At first glance, the e-mail address looks like my own. But the hacker created a new e-mail address that only differed from my own by missing one "l."

Hackers are sophisticated. They'll use your Facebook information to make their stories more believable to your contacts. They'll block your access by changing your account information (e-mail and passwords), and they'll delete your e-mail contacts, making it more difficult to contact your friends and loved ones to warn them of a scam.

And, worst of all, they can do this, unchecked, for days, thanks to Facebook's lack of customer service: the average response time for Facebook to contact law enforcement, following a police report is two to four days, according to Facebook's own automated law enforcement phone line.

Other than automated, generic and unhelpful messages, I have received nothing from Facebook but a lingering silence, which hackers use to their advantage.

Here are some tips to keep your Facebook account, your credit accounts and your e-mail contacts secure, since you very well may be on your own:

Paul Sheppard is the CEO of a2b Technologies, a Web development and information technology company in Elkins Park, and is my favorite computer geek. His advice? He says to use anti-virus software to keep hackers out of your online world. Hackers can use a keylogger, for example, to obtain keystrokes that include your bank accounts, online credit card purchases, logins and passwords.

Facebook has updated its security by giving users the ability to add a second e-mail address and a mobile number that send you alerts via text message. This feature can inform you when a new computer accesses your account.

Sheppard also suggests using a strong password that is eight characters or more long and uses a combination of uppercase and lowercase letters as well as numbers and non-dictionary words. He also recommends using different passwords for each account, and changing each password frequently and never opening a link or attachment you don't recognize.

The Federal Trade Commission's instructions for protecting yourself from identity theft include placing a fraud alert on your credit reports, and reviewing your credit reports by contacting the three credit bureaus: TransUnion: 1-800-680-7289, www.transunion.com; Equifax: 1-800-525-6285, ww.equifax.com; or Experian: 1-888-EXPERIAN (397-3742).

The FTC also maintains a toll-free Identity Theft Hotline at: 1-877-ID-THEFT (438-4338).

After badgering Facebook daily for three weeks via e-mail and phone messages, I was able to re-claim my online profile and pictures. But I wasn't as lucky with my e-mail account; only contacts list was restored.

I still have to worry about whether or not the hacker will try to use my information in the future. So be warned, be safe. Protect yourself, your contacts and your precious photos, so you don't fall prey to an unscrupulous hacker.