Lessons Learned From the Yahoo Security Breach

The recent Yahoo data breach -- characterized by some as the biggest hacking incident in history -- is the latest reminder of just how widespread cybercrime is, and how vulnerable your personal data is when conducting business and communicating online.

As the name implies, social engineering relies heavily on human interaction and often involves tricking unsuspecting victims into breaking normal security procedures.

The attack, which is said to have taken place two years ago, is estimated to have affected at least a half billion Yahoo accounts, exposing user email addresses, phone numbers, birth dates, as well as other personal information. Yahoo, which alleges the attack was carried out by an unnamed foreign government, has come under fire for not discovering and reporting the breach when it originally happened back in 2014.

Since the hack was revealed, the online giant has taken steps to protect its users, including revoking security questions and answers, yet security experts say it will take months before it starts to rebuild user trust.

Cyber Crime: A Rapidly Shifting Model

According to the Federal Trade Commission (FTC), over 490,000 consumer complaints about identity theft were received by the agency in 2015, representing a 47% increase over the prior year.[1] For its part, the Department of Justice estimates that more than 17 million Americans were victims of some form of identity theft in 2014.[1]

Criminals obtain a victim's personal information in a number of ways -- both online and off. And as incidents of cyberattacks grow, so too does the arsenal of tools and sophistication level of techniques used to perpetrate the crimes.

One such technique is social engineering. As the name implies, social engineering relies heavily on human interaction and often involves tricking unsuspecting victims into breaking normal security procedures. In short, it is a way for criminals to gain access to your computer or mobile device and the sensitive personal data it stores.

Phishing, a form of social engineering, uses email to lure victims to fake websites and then gain access to their passwords and usernames, credit card numbers, or other key data. Phishing emails often appear to be from a legitimate company that the victim recognizes.

In yet other instances, attackers may inject malicious code into your computer via emailed attachments and links, infected search engine results, or through videos and documents on legitimate websites, particularly social networking sites.

In the mobile device world, criminals can corrupt a legitimate smartphone app and upload it to a third-party site. If users innocently install the app, they expose their devices to assaults by hackers who collect personal user data, change device settings, and sometimes even control the device remotely.

Don't Be a Victim

In today's 24/7/365 world, it is nearly impossible to secure all sources of personal information that may be "out there" waiting to be intercepted by eager thieves. But you can help minimize your risk of loss by following a few simple rules.

- Use strong passwords. Create passwords of at least eight characters that include a liberal mix of uppercase and lowercase letters, numbers, and special symbols. Security experts recommend using "pass phrases" -- short, random words separated by spaces or other characters, for example "run_full@snow."
- Change passwords often. This falls under the category of "good housekeeping" for your financial accounts. It may seem like a nuisance, but it is one of the easiest ways to help keep cybercriminals from breaking into your online accounts.
- Avoid using the same password for multiple online accounts. If hackers steal your password for one account they can easily gain access to another using the same credentials.
- Use secure websites. When banking or shopping online, be sure to use websites that protect your financial information with encryption. Sites that are encrypted start with "https." The "s" stands for secure.
- Seek two-factor authentication. Some websites, primarily financial institutions, are requiring more than a password to confirm your identity. For example, when placing an order online you may be prompted to enter a one-time code that is sent to you via text message or a phone call. Yahoo is now recommending that users turn on its two-factor authentication tool: Yahoo Account Key. Each time users try to access their accounts, Yahoo will send a confirmation to their phones.
- Check your credit reports. Make a habit of checking your credit reports at least once a year -- and much more frequently if you fear or have been informed that your credit or debit card has been involved in an online scam. Each of the big three credit reporting agencies -- Experian, TransUnion, and Equifax -- provides a free annual report. Just go to annualcreditreport.com to request your free reports.
- Use fraud alerts. You can also go directly to each of the three reporting agencies (contact information listed below) and request that a free fraud alert be put on one or more accounts.

- TransUnion: 1-800-680-7289; transunion.com; Fraud Victim Assistance Department, P.O. Box 2000 Chester, PA 19016-2000
- Equifax: 1-800-525-6285; www.equifax.com; Fraud Victim Assistance Department, P.O. Box 740256, Atlanta, GA 30374-0241
- Experian: 1-888-EXPERIAN (397-3742); experian.com; National Consumer Assistance, P.O. Box 9554, Allen, TX 75013

A free alert can last up to 90 days but can be extended -- if the situation warrants -- for up to seven years. The Federal Trade Commission's Consumer Information website will walk you through the Fraud Alert process step by step.

[1]The Federal Trade Commission, news release, "FTC Announces Significant Enhancements to IdentityTheft.gov," January 28, 2016.