Digital Deception: Current Trends in Cybercrime

In December 2016, Yahoo announced that data associated with more than 1 billion user accounts had been stolen in 2013. The company believes this was a separate incident from a previously announced theft of data from 500,000 user accounts in 2014.[1] Although the sheer number of compromised accounts is staggering, the Yahoo breaches are just two out of many major data breaches discovered in 2016, ranging from dating sites and Internet companies to the IRS and the U.S. Department of Justice.[2]

Private companies and government agencies that hold personal information are responsible for protecting that data, but even the most vigilant organization can be vulnerable. Moreover, once a data breach has occurred, "aftershock" breaches can continue for years as cyber thieves exploit stolen information. Here is an overview of current cybersecurity trends and steps you can take to help protect your identity and personal accounts.

Passwords and Security Questions

An analysis of 10 million stolen passwords found that the most common password — used by 17% of users — was 123456.[3] Many of the other top passwords were simple combinations of numbers or letters that could be cracked in seconds by dictionary-based hacking software. A strong password should be at least eight characters long and use a combination of lower-case letters, upper-case letters, numbers, and symbols. Avoid dictionary words and personal information such as your name and address.

You should have a separate password for each account or website, and change passwords frequently. Consider using a password manager, a program that generates strong, unique passwords that you control through a single master password. Keep in mind that security questions can be used to unlock data by thieves who claim to have lost a password. Create answers that are fictional or cannot be discovered by others.

Chips and Strips

The transition to credit cards and debit cards with embedded computer chips utilizing EMV (Europay, MasterCard, and Visa) technology has reduced fraud at checkout terminals in brick and mortar stores. But EMV technology does not protect card numbers used online; in fact, thieves have shifted efforts to digital merchants, which have seen an increase in cyber theft. EMV adoption has also stimulated an increase in new account fraud in which thieves use stolen information to create new accounts with new cards.[4]

The EMV rollout has been slow, and cybersecurity experts predict more widespread use of sophisticated skimmers inserted into a card reader to steal information from magnetic strip cards.[5] Gas stations, a favorite target for skimmers, are not required to install EMV terminals until October 2017. When using a card reader terminal, particularly in a standalone location, be aware of anything that looks amiss, such as colors that don't match or arrows that don't line up. If you are suspicious, do not use the terminal and report the issue immediately.

Mobile Payments

The United States has been slow to adopt mobile payment technology, but 2016 represented a big step forward. Almost 40 million Americans made a "proximity payment" using their mobile phones at the point of sale, and more than 45 million transferred funds with a mobile payment peer-to-peer application.[6]

Paying with your smartphone could be safer than paying with plastic as long as you take the same security precautions you would on your computer and utilize security enhancements such as fingerprint access. Also be aware that hackers have begun to send malware through texts as well as emails.

Health-Care Attacks

According to an IBM security survey, the health-care industry was the top target for cyber criminals in 2015 — with over 100 million records compromised — surpassing the financial services industry.[7] Cybersecurity experts predict that medical cybercrime will accelerate and spread to larger networks in 2017.[8]

For consumers, stolen medical information can lead to fraudulent and expensive claims, and collateral damage as thieves use personal data in electronic medical records to open other accounts.

Protect your health insurance ID card as you would a credit card, and monitor explanations of benefits (EOBs) from your insurance company and payment records from health savings accounts.

What Can You Do?

Here are some other security tips to help protect your identity.

Take an extra step. Two-step authentication, such as a text or email code along with your password, could help protect your sensitive data.

Monitor your accounts. Notify your financial institution immediately if you see suspicious activity. Early notification not only can stop the thief but may limit your financial liability.

Think before you click. Never click on a link in an email or text unless you know the sender and have a clear idea where the link will take you.

Shop secure. When shopping online, look for the secure lock symbol in the address bar and the letters *https:* (as opposed to *http:*) in the URL.

Minimize information. Provide only as much information as necessary for your purpose. If you are suspicious of any request for information, don't provide it.

Protect your Social Security Number. Your SSN is the key to a whole world of personal information. Do not carry your card in your wallet and never provide your number online unless you are on a secure IRS or Social Security Administration website.

1) Yahoo, December 14 and September 22, 2016
2) IdentityForce.com, 2016
3) *Security*, January 13, 2017
4) Javelin Strategy & Research, 2016
5, 8) Experian, 2016
6) eMarketer, November 7, 2016
7) IBM, 2016