Here’s How Your Identity Will Be Stolen: The Top 10 Scams

April 18, 2012 - TIME Moneyland

By Martha C. White | April 5, 2012 |

1. Phishing

**The Scam:** You get an email purportedly from your bank, credit card provider or utility company. Often, it will say there’s some emergency or that there’s an issue with your account. The messages include a link that takes you to a fake version of the company’s website, with a login prompt that exists solely to capture your user name and password. With access to your account, a crook can peek inside and get your mailing address and any associated account numbers.

**Avoid It By:** If you get an urgent-sounding message from any company, especially a financial institution, that you do business with, don’t click on anything. Go to the company’s site directly and call or email to verify that the message is legit.

2. Pretexting

**The Scam:** This works exactly the same as phishing, but it’s done over the phone. “People pose as legitimate businesses to trick you into giving out information,” says John Everett, spokesman for the National White Collar Crime Center. The caller pretends to be from your bank, credit card company or even a government agency and tells you there’s some issue that can only be resolved if you provide account information, your Social Security number, login credentials or the like.

**Avoid It By:** Alarms should start ringing in your head if anybody calls you out of the blue and starts asking for this kind of info. Hang up on them and call wherever they were supposedly calling you from, both to establish that there is no problem with your account and to tip them off to the scam so they can warn other customers.

3. Fake Job Offers

**The Scam:** The Better Business Bureau of New York flagged this as number one on its roundup of the top scams of 2011. You respond to a job ad, often a “work from home” type of deal, and are told you’ve been hired after a phony phone interview. Some of these crooks go so far as to create a fake company website and other flourishes to make this look
legitimate. Then they’ll ask for a Social Security number for a “credit check” or bank account information “to set up direct deposit,” which is just a ruse to steal your information.

Avoid It By: No matter how long or how grueling your job search is, do some due diligence online, over the phone and, when possible, in person on any employment offers.

4. Skimming

The Scam: A “skimmer” is a small, unobtrusive device that reads the information on a credit or debit card’s magnetic strip. In some cases, crooks install them in gas pumps or at ATMs, turning a routine transaction into an assault on your privacy. Skimming can also occur in retail situations, often restaurants, where a server will swipe your card through a handheld skimmer before running it through the establishment’s legitimate card reader. With the stolen data, identity thieves manufacture fake credit cards.

Avoid It By: Don’t swipe your card at any machine that looks tampered with or otherwise sketchy. If you’re eating out and are concerned about the risk of skimming by waitstaff, bring your card up to the register so it doesn’t leave your sight.

5. Dumpster Diving

The Scam: Like raccoons, crooks aren’t above rooting through garbage looking for goodies. “They rummage through trash looking for bills or other paper with your personal information on it,” the FTC warns in an online publication focusing on identity theft. This method of stealing information is old-school, but experts say criminals still use it because it still works.

Avoid It By: Shred personal documents and credit card offers before throwing them away, and wipe hard drives clean before you get rid of computers or smartphones.

6. Pickpocketing and Purse-Snatching

The Scam: This isn’t really a scam so much as old-fashioned robbery, but identity theft experts say it’s still one of the top ways people become victims.
Avoid It By: In addition to the usual personal safety precautions like being aware of your surroundings and observing suspicious behavior, you can cut down on the risk that your data will be used fraudulently. Keep a copy of the customer service numbers of your credit and debit cards someplace accessible so you can alert issuers to freeze your accounts. If you have a smartphone, install an application that lets you erase it remotely, so a thief can’t access any information stored there. And never, ever keep your Social Security number in your wallet. “If your wallet or purse is lost or stolen with your Social Security number and your driver’s license, that is a jackpot for a criminal that wants to steal your ID,” Everett says.

Malware and Spyware

The Scam: Clicking on a pop-up or a link in an email can unleash a program that sneaks into your computer and records your keystrokes: user names and passwords, account numbers, addresses — it captures everything and sends it back to the perpetrator, who now has everything he or she needs to steal your identity. Adam Levin, co-founder and CEO of Identity Theft 911, says cybercrooks are now creating similar tools to steal data via smartphone apps. “Fraudsters can gather data and intercept browsing sessions on your smartphone to gather information,” he says.

Avoid It By: Keep anti-virus, malware and spyware protection on your desktop or laptop up-to-date, and don’t click on pop-ups or links from unknown email senders. Protect your smartphone by only downloading apps that are part of that platform’s official marketplace.

8. Fake Tax Filing

The Scam: As if filing your taxes isn’t arduous enough, some people get an unpleasant surprise when they find out an identity thief has already claimed their refund. In some cases, cybercrooks use stolen personal information to file a fake return, then transfer “your” money onto a prepaid debit card. More rarely, scammers trick you into handing over your information. The Better Business Bureau issued a warning about this practice: Victims would get emails claiming that their tax information was incomplete. The emails would include a link that would take them to a fake IRS site that prompted them to enter their personal information.

Avoid It By: The IRS doesn’t contact taxpayers by email; any such solicitation is a fake. "An IRS notice informing a taxpayer that more than one return was filed in the taxpayer’s name or that the taxpayer received wages from an unknown employer may be the first tip off the individual receives that he or she has been victimized,” the agency’s website says. If you get one, contact them right away.
9. Change of Address

The Scam: A criminal can get billing statements, bank account information and credit card offers by misdirecting your mail. "They divert your billing statements to another location by completing a change of address form," the FTC’s website says. Not only could you have your identity stolen, but you could also miss crucial payment deadlines and other mail.

Avoid It By: Shred mail — even junk mail — that might tempt a crook (such as credit card offers) and pay attention to what's in your mailbox. If you get a notice informing you about a change of address and you haven’t moved, get in touch with the post office. If you suddenly stop getting statements from your bank or credit card company and you haven't gone paperless, call them to make sure someone isn't impersonating you via mail.

10. Data Breaches

The Scam: With the growing amount of information stored and transmitted digitally by banks, credit card companies and other third parties, there are more loopholes for a clever hacker to exploit. The recent Global Payments breach that affected Visa and MasterCard customers is just the most recent. In the past, banks, merchants and even online gaming platforms have been broken into. What’s more, with the rise of “hactivism” as a form of protest, personal data is collateral damage.

Avoid It By: Unfortunately, there’s not much most of us can do to prevent this. We depend on the companies with which we do business — and the companies they do business with — to keep our data safe. Since one item often stolen is passwords, create different passwords for your online banking, shopping and so on. This at least keeps a one-time breach from snowballing.