Stanford Center on Longevity

A **TOOLKIT** SERIES BRIEF

AVOIDING FRAUD 101

Cyber Safety Tips to Avoid Scams

Marti DeLiema
Postdoctoral Scholar
Financial Security Division
Stanford Center on Longevity

STANFORD CENTER ON LONGEVITY

TAKE-HOME POINTS

- The internet has revolutionized the way we communicate with each other, seek information and purchase goods and services.
- While it's easier than ever to connect with those around us, financial predators exploit our reliance on the internet by impersonating the people and websites we trust.
- The goal of these scammers is to fool us into giving them money or divulging our personal information in an anonymous space.

This toolkit brief describes important strategies for keeping your personal information safe from online predators.

In addition to communicating and accessing information, we also use the internet to purchase products and services. While most of what we see and buy online is legitimate, according to a 2013 Federal Trade Commission survey on fraud in the U.S., nearly 40 percent of fraudulent items were sold to people online[1] (see Figure 1).

Scam artists don't need to use "brute force" hacking to steal our financial and personal information from our devices. Rather, they cleverly trick us into willingly handing over this information using phishing tactics and social engineering. Most of us are probably familiar with, and likely have received, spam messages from a "Nigerian prince" or a warning that our password is about to expire. Another popular fraudster trick is directing users to fake websites that mimic legitimate ones owned by banks, credit card companies, government agencies and healthcare institutions. The fraudsters' hope is that unsuspecting marks will enter passwords and account information on the counterfeit site before realizing it's a fake. Other scams involve free software downloads that have hidden viruses, fake items posted for sale on sites like Craigslist and eBay, bogus online dating profiles and spam messages claiming the recipient has won a windfall of money or that a friend is in jail in a foreign country. While internet scams take many forms, following the security practices outlined below will help keep consumers protected from a variety of cyber attacks.

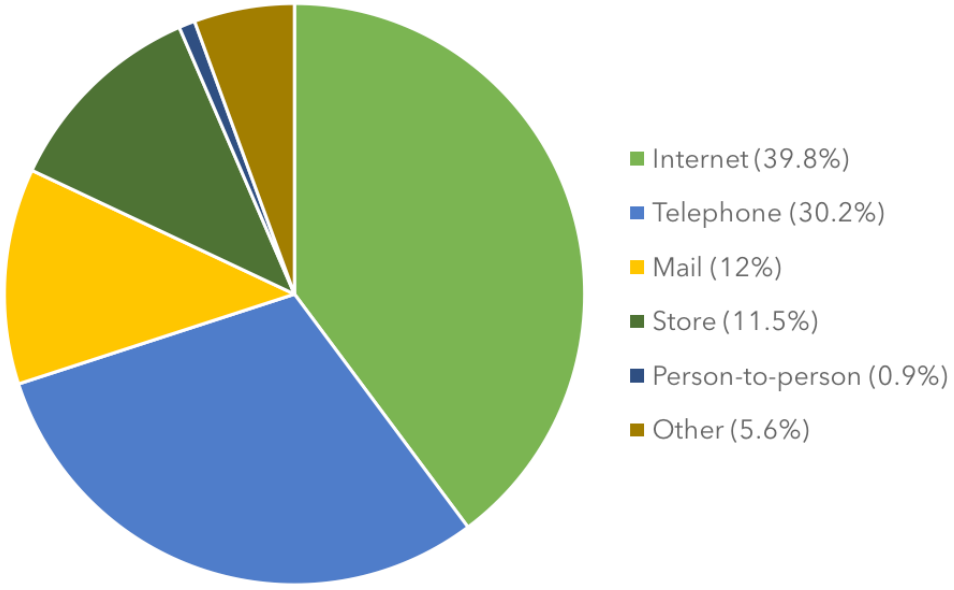

FIGURE 1 Most consumers send money to fraudsters using the internet.

Source: Federal Trade Commission, 2013

DON'T REPLY TO EMAILS ASKING FOR PERSONAL INFORMATION.

Legitimate organizations will never ask a customer to send personal information or account details in an email or text message. Financial institutions and government agencies provide secure channels for people to send personal data, such as birthdates, addresses, phone numbers, account numbers and Social Security numbers. If you receive an email or text request to "validate" or "update" your information, call the person or organization directly instead of hitting "Reply." And don't call the number listed in the original message. Search for the organization online, or get their phone number from an old account statement.

INSPECT A WEBSITE'S URL.

Look for the lock icon that appears next to a website's URL at the top of the internet browser in the status bar. This lock symbol and the "https:" at the beginning of a web address indicate the site is secure and that your information is encrypted when it's transmitted (the "s" at the end of "https:" stands for secure). Verifying the URL is particularly important when entering payment or account information online. Unfortunately, clever fraudsters have found ways to forge a website's security certifications so while this strategy isn't foolproof, it will help you avoid the majority of counterfeit sites. Also, always use a credit card for online purchases instead of a debit card. Credit cards have more security controls in place and give consumers a window to contest fraudulent charges to get their money back.

IF YOU DON'T RECOGNIZE IT, DON'T CLICK ON IT.

Never open hyperlinks or attachments in unsolicited emails or text messages, even if the message looks like it's coming from a friend or co-worker. These links may contain malware or redirect you to counterfeit versions of legitimate sites. Tricks like these are called phishing scams because the fraudsters are trying to bait you into clicking. Similarly, be wary of any "free" software downloads. Carefully check the developer and the source before installing anything on your computer.

Popups are advertising messages used to grab users' attention and redirect them from one website to another. Aside from being annoying, some popup ads contain malware, which can include software that installs hidden viruses on your computer, spyware that monitors your internet usage and Trojan horses like keystroke loggers that secretly record which keys you press. Fraudsters use that information to steal passwords and other confidential data. You can enable (turn on) popup blockers on your internet browser to prevent popup windows. This is a standard option on most browsers, including Mozilla Firefox, Internet Explorer, Safari and Google Chrome. You may need to disable the popup blocker to use a specific online program, but then you should turn it back on as soon as that activity is complete or only allow popups on a site-by-site basis.

GET CREATIVE WITH YOUR PASSWORDS.

Creating a variety of passwords and changing them frequently is a hassle, but it's the best way to make sure fraudsters stay out of your online accounts. The box below has some password advice to keep you from being an easy mark.

TIPS FOR CREATING ROBUST PASSWORDS

1. Create passwords that are a mix of letters, numbers and symbols.
2. Choose a password that is a minimum of eight characters long.
3. Don't reuse the same password for different sites. If hackers gain access to one of your online accounts, it will be easy for them to access others.
4. Change your passwords every three months or so. Come up with your own strategy for creating unique passwords that only you would know.
5. Always change the default password that's provided to you automatically if you forget your log-in information and need to request password help.
6. Never give your password to anyone over the phone or in an email. Your passwords are for you and you alone. Not even the company that manages your account should know your password.
7. Disable stored passwords from your browser. If your computer is hacked, fraudsters may be able to find where all your login information is stored.

SAFEGUARD YOUR DEVICES.

Make sure you have virus protection software installed on all your computers and that it's up-to-date. Antivirus software scans devices for malicious files that slow down processing speed, destroy data, cause programs to crash or spy on users. There are a lot of virus protection software options on the market. Some programs are free to install, but you should verify their legitimacy before downloading. Also, make sure all your social media accounts are set to "private" to ensure that strangers can't easily discover your pictures and posts meant only for friends and family to see.

> Frauders' exploit strategies and phishing tactics will continue to change as new technology enters the market place and we rely more and more on the virtual world.

SET UP AN ONLINE BANK ACCOUNT.

It's a smart idea to create online accounts for each of the financial institutions you deal with, including your bank, credit card companies and investment firms. You don't actually have to use the online services of these institutions, but creating the accounts yourself blocks financial predators from doing it for you. Use unique usernames and passwords for each of these accounts, and monitor your account statements regularly to make sure nothing has been compromised.

BACK UP YOUR FILES REGULARLY.

Nothing is more devastating than losing important documents, photos or work files because you were a victim of ransomware fraud. Ransomware is a popular online scam whereby fraudsters infect your computer with malware that either encrypts your data or locks you out of your operating system, which blocks you from accessing files. Then, if you don't pay the fraudsters the ransom they demand, usually somewhere between $500 and $1,000, they'll destroy the data stored on that device; your pictures, audio files, applications and documents will all be lost. To help protect these files, it's essential to back up your computer by saving your files and applications on an external hard drive or in a cloud account.

SUMMARY

Fraudsters are growing more sophisticated in their methods, even outsourcing the tools and technologies they need to deceive internet users. Their exploit strategies and phishing tactics will continue to change as new technology enters the marketplace and we rely more and more on the virtual world. While none of the strategies presented in this brief are foolproof, integrating them into your online behavior will help reduce the risk of fraud and identity theft.

ACTION STEPS

Here are some helpful online resources for avoiding internet scams:

1. Online safety tips from the Federal Trade Commission: https://www.consumer.ftc.gov/topics/online-security
2. AARP's "Internet Security: Stay Safe Online" guide: http://www.aarp.org/money/scams-fraud/info-08-2011/internet-security.html
3. Types of internet fraud to look out for: https://www.usa.gov/online-safety
4. File a cyber fraud report to the Internet Crime Complaint Center (IC3): https://www.ic3.gov/complaint/default.aspx

CITATIONS

1. Anderson, K. B., *Consumer Fraud in the United States, 2011: The Third FTC Survey*, Federal Trade Commission (2013).

The mission of the Stanford Center on Longevity is to redesign long life. The Center studies the nature and development of the human life span, looking for innovative ways to use science and technology to solve the problems of people over 50 in order to improve the well-being of people of all ages.

Stanford Center on Longevity | Stanford University | 365 Lasuen St | Stanford, CA 94305

STANFORD CENTER ON LONGEVITY