IDENTITY THEFT AND INTERNET SCAMS TIP CARD

Now, more than ever, people are sharing sensitive personal information about themselves online. Technology allows us to connect to each other around the world no matter our location, bank and shop online, and even control our televisions, homes, and cars from our smartphones. With this added convenience comes an increased risk of identity theft and Internet scams. Every time we connect to the Internet – at home, at school, at work, or on our mobile devices – we make decisions that affect our cybersecurity.

DID YOU KNOW?

- Roughly half of American adults (110 million) had their personal information exposed by cybercriminals in 2015 alone.[1]
- Two-thirds of Americans (65 percent) who use the Internet received at least one online scam offer during 2013.[2]
- Identity theft has been at the top of the Federal Trade Commission's Top Consumer Complaints list for 15 years in a row.[3]

COMMON INTERNET SCAMS

Just as technology continues to move forward, making our lives easier and more connected, cybercriminals will use more sophisticated techniques to exploit technology to steal your identity, your personal information, and your money. To help protect yourself against online threats, here is a list of common Internet frauds from the Federal Trade Commission.

- **Identity theft** is the illegal use of someone else's personal information in order to obtain money or credit. How will you know if you've been a victim of identity theft? You might get bills for products or services you did not purchase. Your bank account might have withdrawals you didn't expect. You may see unauthorized charges on your credit cards. You may even see new accounts opened in your name that you did not authorize. You may fail to receive regular bills or mail. You may be unexpectedly denied for a credit application (when you believe you should qualify).

- **Phishing attacks** use email or malicious websites to collect personal and financial information or infect your machine with malware and viruses. Cybercriminals use legitimate-looking emails that encourage people to click on a link or open an attachment. The email they send can look like it is from an authentic financial institution, e-commerce site, government agency, or any other service or business.

- **Imposter scams** happen when you receive an email or call seemingly from a

---

[1] Ponemon Institute, "2015 Cost of Cyber Crime Stud: Global", 2015.

[2] AARP, "Caught in the Scammer' Net Risk Factors That May Lead to Becoming an Internet Fraud Victim", 2014. [3] Federal Trade Commission, Top Complaints, 2014.

government official, family member, or friend requesting that you wire them money to pay taxes or fees, or to help someone you care about.

- **"You've Won" scams** occur when you get an email telling you that you have won a prize, lottery, or sweepstakes. Though the person seems excited for you to collect your winnings, they then tell you there is a fee or tax to pay for the prize and request your credit card or bank account information.

- **Healthcare scams** happen when you receive a call, email, or letter that promises big savings on health insurance but claims that you need to provide your Medicare or health insurance information, Social Security number, or financial information to take advantage of the deal.

SIMPLE TIPS

There are many steps consumers can take to avoid becoming victims of identity theft or online scams.

- **When in doubt, throw it out.** Links in email, tweets, posts, and online advertising are often the way cybercriminals compromise your computer. If it looks suspicious, even if you know the source, it's best to delete it. You also have the option, if appropriate, to mark it as "junk email" so you no longer receive emails from this sender.
- **Think before you act.** Be wary of communications that implore you to act immediately, offer something that sounds too good to be true, or ask for personal information.
- **Make passwords long and strong.** Create a password with eight characters or more that uses a combination of numbers, letters, and symbols.
- **Guard your personal information.** Keep Social Security numbers, account numbers, and passwords private, as well as specific information about yourself.
- **Use stronger authentication.** Using stronger authentication requires that you use your password in conjunction with an additional piece of information (such as a PIN sent to your mobile device) to verify your identity. Even if a cybercriminal is trying to access your account and has captured your password, they still cannot get account access without the second component, if you have instituted stronger authentication. Visit www.lockdownyourlogin.com for more information on stronger authentication.
- **Unique account, unique password.** Create unique passwords for each account. Keeping separate passwords for every account helps thwart cybercriminals.

PROTECT YOURSELF FROM ONLINE FRAUD

When seeking the following information online, you can take precautions to protect yourself from fraud:

Banking

- Avoid accessing your personal or bank accounts from a public computer or public Wi-Fi network, such as the public library. Not only can cybercriminals potentially gain access to your accounts through public Wi-Fi, but strangers can easily shoulder surf and see the sensitive information on your computer or mobile device screen.
- Don't reveal personally identifiable information such as your bank account number, Social Security number, or date of birth to unknown sources.

- When paying a bill online or making an online donation, be sure that you type the website URL into your browser instead of clicking on a link or cutting and pasting it from the email.

Shopping

- Make sure the website address starts with “https”; the “s” stands for secure.
- Look for the padlock icon at the bottom of your browser, which indicates that the site uses encryption.
- Type new website URLs directly into the address bar instead of clicking on links or cutting and pasting from the email.

Medical advice

- Be sure to find out who is providing the information and check that you are visiting legitimate websites when you go online.
- Look for websites ending in .edu (for education) or .gov (for government) for legitimate medical information.

RESOURCES AVAILABLE TO YOU

If you discover that you have become a victim of cybercrime, immediately notify your local authorities to file a complaint. Keep and record all evidence of the incident and its suspected source. The list below outlines the government organizations that you can file a complaint with if you are a victim of cybercrime.

FTC.gov

The Federal Trade Commission’s (FTC) free, one-stop resource, www.IdentityTheft.gov can help you report and recover from identity theft.

Report fraud to the FTC at ftc.gov/OnGuardOnline or www.ftc.gov/complaint

US-CERT.gov

Report computer or network vulnerabilities to US-CERT via the hotline: 1-888-282-0870 or www.us-cert.gov. Forward phishing emails or websites to US-CERT at phishing-report@us-cert.gov.

IC3.gov

If you are a victim of online crime, file a complaint with the Internet Crime Compliant Center (IC3) at http://www.IC3.gov.

SSA.gov

If you believe someone is using your Social Security number, contact the Social Security Administration’s (SSA) fraud hotline at 1-800-269-0271.

Stop.Think.Connect. is a national public awareness campaign aimed at empowering the American public to be safer and more secure online. The Campaign’s main objective is to help you become more aware of growing cyber threats and arm you with the tools to protect yourself, your family and your community. For more information visit www.dhs.gov/stopthinkconnect.

Homeland Security

www.dhs.gov/stopthinkconnect

STOP | THINK | CONNECT™