Consumer Federation of America
1620 I Street, N.W., Suite 200 * Washington, DC 20006

Get Smart: Protect Yourself, Your Friends and Your Family from ID Theft and Fraud

Identity theft is when someone steals your personal information and uses it pretending to be you, usually to get money but sometimes just to be mean. It can happen in many ways, but now that we have so much personal information on our computers, laptops, notebooks and smartphones, these devices are tempting targets for ID thieves. They don't even need to steal your phone or computer – they can get the information it contains without your even realizing it. And if they need more information about you, they may try to trick you into providing it.

What's the harm? ID thieves could wipe out your bank account, open credit accounts in your name or take over existing accounts and wreck your credit record, or alter your health records by posing as you to get medical services. They could also create trouble for you with the IRS by using your Social Security number and other information to get a job. When you file your tax return, you could find that someone else already has, and got a tax refund.

Even worse, if they get into trouble with the law they could give your ID as theirs. If you're stopped for a minor problem like a broken taillight and the cop checks the computer, you could be arrested on an outstanding warrant for something you never did.

And your reputation could be damaged if someone gets into your social network account and posts embarrassing photos or malicious comments, making it look like you did it.

ID thieves can also target your friends and relatives. For instance, if they get into your email or other messaging services they could send desperate-sounding pleas to your contacts saying you've been in an accident or have some other emergency and need money to be wired to you immediately. Of course, it's the scammer who picks up the cash, not you. Another scam is to send your contacts a message pretending to be from you with an attachment or website to click on. Your friends and family trust you, right? So they'll click on it and when they do, nasty programs called malware could be secretly downloaded to their devices to steal their account numbers, passwords, and other personal information. Now *you* are responsible for their becoming victims.

<u>Seven Simple Steps to Protect Yourself and Others from ID Theft and Fraud</u>

1. **Keep your personal information private.** Once it's out there, it may not be possible to retrieve or erase it. Don't post your address, Social Security number, or other very personal information on social networking sites. Use the privacy settings on social networks to limit who you want to be able to see the information you post, and be wary of strangers who want to be your friends, since they

may be fraudsters instead. And only provide your personal information when it is absolutely needed for something – if you're not sure why someone wants it, ask.

2. **Use strong passwords to lock your accounts and your devices.** Sure, using passwords can be annoying, but any barriers you put in front of ID thieves make you a less attractive target. Can't remember your passwords? It's OK to write them down as long as you store them somewhere safe. Create passwords that aren't easy to guess – not your birthday or your pet's name! And not words that are in the dictionary, since crooks can use programs to run through the dictionary in minutes.
3. **It's best not to click on invitations, photos, cards, or websites that are sent by strangers.** They may contain malware. If you receive something like that out of the blue and it looks like it's from someone you know, contact that person to check whether it's legitimate. If you don't recognize the sender, just delete it.
4. **Only download free games, toolbars, icons, file sharing programs or other free stuff from sources you trust.** Otherwise you may end up paying a high price by letting an ID thief into your device.
5. **Watch out for "phishing."** No, it's got nothing to do with the band Phish; phishing is when an ID thief poses as someone you may trust, such as a company you do business with, your employer, your school, even a government agency, and contacts you unexpectedly to ask for your account number, Social Security number, or other personal information. The request may come by email, text, or a phone call and the reason that's given may vary: there's a problem with your account, the files need to be updated, or you're eligible for a new program or benefit. But there's always a sense of urgency – you need to respond right away! Don't. Check directly with whoever the person claims to represent to make sure the request is legitimate.
6. **Use a firewall and malware protection to keep ID thieves at bay.** Many computers and smartphones come with them built in, and you can also find this software for free or for sale on the Internet. Look for reviews from tech magazines and other independent sources.
7. **Be really careful when you're using free public WI-Fi.** It's convenient but it's usually NOT secure. Crooks can use various high-tech means to "eavesdrop" on your email or communications on social networks and read what you're typing. If you're banking or shopping with your device, your account numbers could be exposed. It's more secure if you disable file sharing, only go to websites that are encrypted (your information is turned into code as it is transmitted), and use a virtual private network (VPN). Sound too complicated? It's not, and if you search online for public Wi-Fi safety you'll find many websites where you can learn more about these protections and how to use them. If you're not sure you are secure using public Wi-Fi, wait until you're home or somewhere else with a secure connection, especially to do things that involve your most sensitive personal information.

Sources for More Information

Consumer Federation of America, www.consumerfed.org/idtheft and www.IDTheftInfo.org

The Federal Trade Commission, www.onguardonline.gov

The Identity Theft Resource Center, www.idtheftcenter.org

The National Cyber Security Alliance, www.staysafeonline.org