Fort Rucker Preventive Law Program

LEGAL ASSISTANCE SERIES

Identity Theft

THIS PAMPHLET

Contains basic information on the above.
If you have specific questions, call
255-3482 to make an appointment.

OFFICE OF THE STAFF JUDGE ADVOCATE
FORT RUCKER, ALABAMA 36362

Stop. Think. Click.
Practical Tips for Preventing Identity Theft
from http://onguardonline.gov/stopthinkclick.html and http://www.consumer.gov/idtheft

What is identity theft?
Identity theft is when someone steals your personal information so they can impersonate you. They do this for a number of reasons, including running up bills and committing crimes in your name. Identity theft can wreak havoc with your credit, making it difficult for you to get credit, buy real estate, and find a job for years to come. It can even affect your criminal record.

How do thieves get your personal information?
Phishing and Online Scams

"Phishers" send spam or pop-up messages claiming to be from a business or organization that you might deal with. The message usually says that you need to "update" or "validate" your account information. It might threaten some dire consequence if you don't respond. Links that seem legitimate in an email may direct you to some other place entirely, without your knowledge. NEVER reply to or click on links in emails or pop-ups that ask for personal information. Emails and pop-up windows requesting personal information tend to be fraudulent. Most banks, credit card companies, and online retailers have policies against requesting personal information via email. If you get an email that tells you to click on a link, the safest thing to do is to contact the company referenced directly to ask about the issue. You can either call the customer service number on your account statement, or you can open a new browser window and type the URL into the address field, watching that the actual URL of the site you visit doesn't change and is still the one you intended to visit. Forward spam that is phishing for information to spam@uce.gov and to the company, bank, or organization impersonated in the phishing email. Most organizations have information on their websites about where to report problems.

Email

DO NOT open email attachments unless you recognize and trust the person who sent them to you – AND unless you are sure that that person intended to send the attachment. Viruses often hide in attachments and can seriously damage your computer if the attachment is opened. Once established, they can infect your email address book and send apparently legitimate emails to your contacts to infect their computers as well.

File-Sharing

If you use file-sharing software, make sure you have it set up properly, so other users cannot access your personal files, such as tax returns, emails, medical records, or other personal documents. Be aware that you may unwittingly download illegal material. Read the End User Licensing Agreement to be sure you understand and are willing to tolerate the side effects of any free downloads.

Spyware

Spyware is software installed without your knowledge or consent that adversely affects your computer. Some programs monitor your computer or control how you use it. Even some

legitimate programs come with spyware baggage. Resist the urge to install any software unless you know exactly what it is and what programs it will put on your computer. Consider installing antispyware software, update it regularly, and use it regularly to scan and delete any spyware that might have been installed on your computer.

Documents

Identity thieves will stop at nothing to get your personal information – they'll even rifle through your trash. Make sure you cut up your old credit cards and shred all sensitive documents with a cross-cut shredder before discarding them. Don't forget to shred credit card offers, even if you haven't solicited or opened them. These offers often contain sensitive personal information, and thieves can use them to apply for credit cards in your name.

Tips for Protecting Yourself

1. Protect your personal information. Any time you give out personal information, you are opening yourself up to potential identity theft. If someone requests your name, email or home address, phone number, account numbers, Social Security number, or any other type of sensitive information, make sure you know how it's going to be used and how it will be protected before you share it. Read website privacy policies. Teach your children not to give out any personal information on the Internet. Consider using software with parental controls, but remember that no software can substitute for parental supervision and discussion. Don't fall victim to phishing scams – verify all requests for information. Shred all documents containing personal information with a cross-cut shredder before you discard them.

If you shop online, don't provide personal or financial information through that company's website until you have made sure that the site is secure. Signs of secure websites include a lock icon on the browser's status bar or a website URL that begins "https:" rather than just "http:" Unfortunately, no indicator is foolproof, so be cautious as to which sites you patronize. Another measure you can consider when shopping online is to use a one-time use account number. Many credit card companies will provide an account number for a single purchase that becomes invalid after a short time. Contact your credit card company to ask about this purchase option.

2. Know who you're dealing with. Legitimate online retailers should be able to provide a physical address and a working telephone number at which they can be contacted in case you have problems. Find out which state has registered the business, and check with the Attorney General's office and/or the Better Business Bureau in that state to see whether there have been any complaints against that business.

3. Use antivirus software, antispyware software, and a firewall, and update them regularly. Look for software that recognizes current viruses and malicious programs as well as older ones, that effectively reverses the damage, and has an automatic update option. Firewalls help keep hackers from using your computer to send out your personal information without your permission. Many operating systems and antivirus programs have built-in firewalls, but you have to enable them. There are some excellent free and low-cost antivirus, antispyware, and firewall programs available on the Internet.

4. Make sure your operating system and web browser are set up properly, and update them regularly. Check your browser settings and set them to the highest level of security you can stand without significantly impairing your internet browsing. Update your operating system and browser often. Many operating systems can be set to update themselves automatically. Disconnect or turn off your system when you won't be using it for an extended period.

5. Protect your passwords. Make sure your passwords are hard to guess. A good way of creating a password is to think of a memorable phrase and use the first letter of each word as your password, substituting numbers or symbols for some letters. Use passwords with at least eight characters and that include numbers or other symbols. Don't use common words, your login name, adjacent keys on the keyboard, or your personal information as passwords. Change your passwords at least every 90 days. Use a different password for each online account.

6. Back up important files. Use an external hard drive, memory stick, thumb drive, or some other removable medium to back up your files. Keep your back-up copies in a secure place and update them regularly.

7. Learn who to contact if something goes wrong online.
If your computer gets hacked or infected by a virus:
Immediately unplug the phone or cable line from your machine. Then scan your entire computer with fully updated anti-virus software and update your firewall. Take steps to minimize the chances of another incident. Alert your internet service provider (ISP) and the hacker's ISP (if you can tell what it is). You can usually find an ISP's email address on its website. Include information on the incident from your firewall's log file. Contact the FBI at www.ifccfbi.gov.

Report internet fraud to the Federal Trade Commission at http://ftc.gov.

If you get deceptive spam, including phishing attempts, forward it to spam@uce.gov. Be sure to include the full header of the email, including all routing information. You can also report phishing email to reportphishing@antiphishing.org.

If you think you have mistakenly given your personal information to a fraudster, file a complaint at http://ftc.gov and then visit the Federal Trade Commission's Identity Theft website at www.consumer.gov/idtheft to learn how to minimize your risk of damage from a potential theft of your identity.

8. Place an active duty alert on your credit report during deployments. Military personnel away from their usual duty stations can place an active duty alert on their credit reports to help minimize the risk of identity theft while deployed. They are valid for one year and can be renewed after that year is up. An active duty alert removes you from the credit reporting companies' marketing list for pre-screened credit card offers for two years unless you request otherwise. Contact any one of the three consumer reporting companies listed below to place the active duty alert on your credit report.

9. Monitor your credit reports. You are entitled to a free copy of your credit report from EACH of the three consumer reporting companies EVERY year. http://www.annualcreditreport.com

Take advantage of this. Make sure all the information on your credit reports is accurate. Follow up with your creditors if bills do not arrive on time.

If You Think Your Identity Has Been Stolen

Contact the fraud departments of any one of the three consumer reporting companies, Equifax, Experian, and TransUnion, to place a fraud alert on your credit report. The company you contact is required to alert the others. Contact your creditors, by phone and in writing, to inform them of the problem. Contact your bank and ask them to flag your accounts and to contact you to confirm unusual activity.

Close the accounts that you know or believe have been tampered with or opened fraudulently, and change your PINs and passwords on any accounts you keep open. Use the ID Theft Affidavit available at http://www.consumer.gov/idtheft when disputing new unauthorized accounts.

File a police report in your local community or in the community where the identity theft took place. Submit a copy of the report to your creditors and others that may require proof of the crime. File your complaint with the Federal Trade Commission at 1-877-438-4338 or online at http://www.ftc.gov/ftc/complaint.htm. Keep a log of all contacts and make copies of all documents.

Contact the state office of the Department of Motor Vehicles to see if another license was issued in your name. If so, request a new license number and fill out the DMV's complaint form to begin the fraud investigation process.

If you think your social security number has been stolen, contact the Social Security office at 1-800-269-0271. Submit a copy of your credit report and copies of any of the affidavits that you have filed with the credit bureaus and inform them that your social security number was stolen and that it is having a negative impact on you. The Social Security office will investigate and reissue you a new social security number, if appropriate. Note that you might have some issues getting loans until you reestablish your credit with the new social security number.

You may also want to contact the Privacy Rights Clearinghouse at 619-298-3396 or www.privacyrights.org to network with other identity theft victims.

Consumer Reporting Companies

Equifax: 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241
Experian: 1-888-397-3742; www.experian.com; P.O. Box 9532, Allen, TX 75013
TransUnion: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

Other Resources

http://onguardonline.gov
http://www.consumer.gov/idtheft
http://ftc.gov