Office of the Chief Information Security Officer
Risk Advisory: Identity Theft

BACKGROUND

Having your identity stolen can be intrusive, scary, and have lasting and damaging effects on your finances, medical records, and reputation. Learn what you can do to prevent identity theft and what to do if you become a victim.

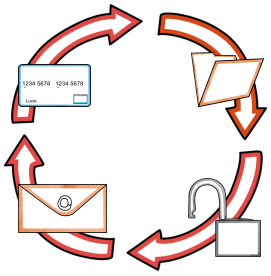
Identity theft is the illegal appropriation of another individual's personal information. It is often used to carry out financial transactions, such as purchases, using a credit card number or taking out a loan, using a victim's name, Social Security number and credit history. Identity theft can also be used to file fraudulent tax returns, acquire medical insurance, or open phone or wireless services and accounts.

Identity thieves obtain personal data in various ways, including looking through trash bins for documents and hacking into organizational systems to steal personally identifiable information (PII).

BEST PRACTICES

Fight identity theft by taking the following precautions:

PERSONAL OR FINANCIAL INFORMATION



- Be skeptical of any email message that asks for personal or financial information.
- Avoid sharing personal information about yourself (such as birthdate, place of birth, family members' names) on social networking websites.
- Shred credit card receipts, junk mail, and other documents with sensitive, financial, or personally identifiable information. Never leave these types of documents in shared spaces, such as on an office fax or printer.
- Monitor your account statements regularly for unauthorized transactions and check your credit report from all three bureaus annually. You are entitled to a free credit report from the three major reporting companies once a year.

Office of the Chief Information Security Officer
Risk Advisory: Identity Theft

EMAIL LINKS AND ATTACHMENTS

- Use caution with all emails containing links or attachments -- even if the sender is someone familiar to you. Email addresses can be spoofed to resemble people you know. Never click on links sent in unsolicited emails.

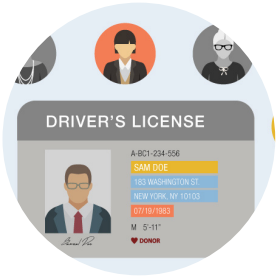
PASSWORDS

- Always use strong passwords or a passphrase that uses a combination of numbers, lower-case and upper-case letters, and symbols.
- Change your passwords frequently, never share them, and don't use your UW NetID password for other accounts.

SOFTWARE

- Apply all critical software patches to keep operating systems and applications up to date. This will help ensure that you receive security updates that protect machines and devices from data-stealing threats such as malicious software (malware).
- Use anti-virus software and keep it updated to protect devices from the latest versions of malware.
- Avoid using software downloaded from unknown websites or peer-to-peer file-sharing services as they may include spyware.

WHAT TO DO IF YOU ARE A VICTIM OF IDENTITY THEFT



- Visit the Washington State Office of the Attorney General's website on identity theft for information and guidance on how to be prepared to respond and report the incident.
- Visit the Federal Trade Commission's website on identity theft for further information, and to report identity theft