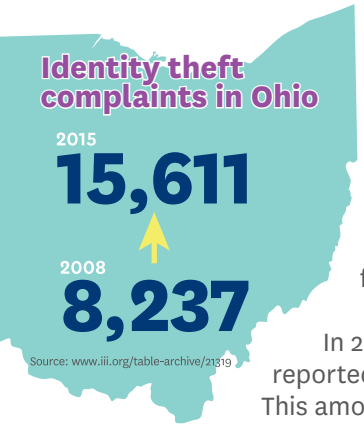
Fall 2017
Cyber Security
Newsletter

KENT STATE UNIVERSITY
Division of Information Services

Protecting Your Identity
in the Digital Age

Each year, an estimated 17.6 million Americans are victims of identity theft.



Identity theft occurs when someone uses another person's personally identifiable information (PII) – such as date of birth, Social Security number, or credit card numbers – to commit fraud or other crimes. In almost all cases, identity theft victims experience some type of financial loss.

In 2014, the average financial loss reported by identity theft victims was $7,761. This amount does not include any costs incurred like legal fees, late-payment penalties, or the purchase of identity protection services.

How does identity theft happen?

Now that we store and transmit most of our information digitally, there are a more ways a thief can obtain PII. An organization's computer network can be compromised to collect thousands of records at once. However, some of the easiest attacks, such as phishing emails*, involve tricking individuals into giving up their PII. Since tricking an individual is often easier than tricking a firewall, these types of attacks are extremely common.

How do I protect my identity?

The longer a criminal has access to personal information, the more damage they can do. A study conducted by the Bureau of Justice Statistics* showed that nearly half of identity theft victims were not aware of any suspicious activity on their accounts until they were contacted by their financial institution.

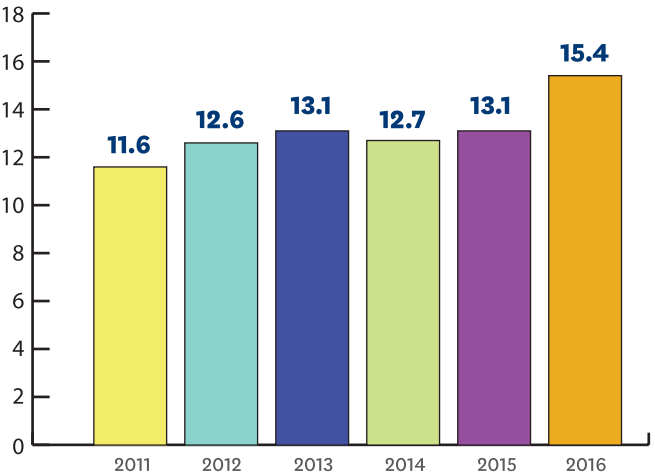
One of the most important steps is to monitor your accounts so that you know if your identity is compromised. Take advantage of free services provided by your bank, credit card companies, and other institutions that give you notifications when transactions occur. You can also subscribe to fee-based commercial products to monitor your accounts and credit rating.

Warning signs

Below are some warning signs of possible identity theft according to the Federal Trade Commission.**

- You receive notice that your information was compromised by a data breach at a company where you do business or have an account
- Withdrawals from your bank account you can't explain
- Expected bills (or other mail) are not received
- Your checks or credit cards are declined
- Debt collectors call you about debts that aren't yours
- Unfamiliar accounts or charges appear on your credit report

U.S. Fraud Victims *(in millions)*



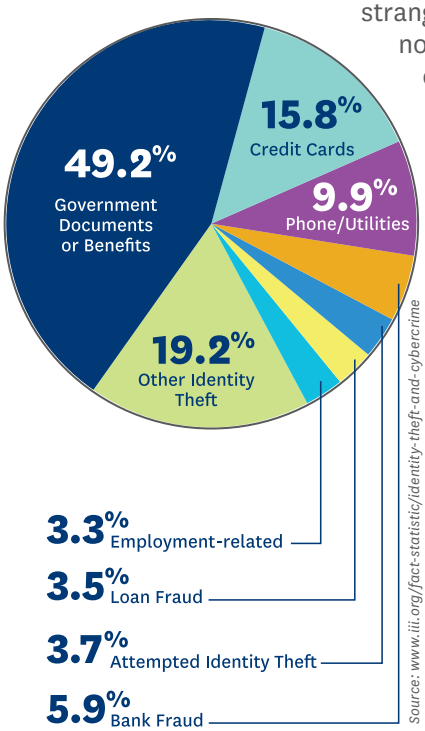
Source: www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new

Security recommendations

The following are some recommendations for securing your identity online.***

Be alert for impersonators and scams
Verify any organization that requests your personal or financial information. If you receive an unsolicited phone call or email requesting this information, be especially wary. Call an official listed number to verify the request.

How victims' information is misused



Learn to Identify Phishing Emails
Do not open files, click links, or download programs sent by strangers or that you were not expecting. Be cautious of emails that urgently require action or request you provide your personal information or passwords. Verify the request by contacting the person or organization from which the email appears to originate.

Use best practices for password management
Create strong, unique passwords and keep them to yourself. Even the strongest passwords are vulnerable if they are shared.

Identity thieves have stolen over
$107 BILLION
in the past 6 years
Source: www.iii.org/fact-statistic/identity-theft-and-cybercrime

Don't Overshare on Social Media
Sharing too much personal information can enable an identity thief to learn enough about you to answer security questions for your accounts. You should never share your account numbers, Kent State ID, or any part of your Social Security Number. Be especially cautious about sharing information like your address or birthday as these pieces of information are frequently used to verify your identity with organizations.

What to do if you suspect identity theft

If you think you are a victim of identity theft, there are several actions you should take immediately. Listed below are the Federal Trade Commission's recommendations.

- Contact the companies where you know fraud occurred and request that they freeze your accounts
- Place a fraud alert on your credit accounts and request a credit report
- Report the theft to the Federal Trade Commission
- File a police report with your local police department

More information about resolving identity theft can be found at **identitytheft.gov**. ☐

* *www.bjs.gov/content/pub/press/vit14pr.cfm*
** *www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft*
*** *www.consumer.ftc.gov/articles/0272-how-keep-your-personal-information-secure*

KENT STATE UNIVERSITY

Division of Information Services

For information about Cyber Security at Kent State, visit **SecureIT.kent.edu**, or contact the Office of Security and Access Management at **security@kent.edu** or **330-672-5566**.

Report suspected scam emails to **phish@kent.edu**.