What is Identity Theft?

Identity theft occurs when criminals steal a victim's personal information to commit criminal acts. Using this stolen information, a criminal takes over the victim's identity and conducts a range of fraudulent activities in their name.

Cyber criminals commit identity theft by using sophisticated cyber attack tactics, including social engineering, phishing, and malware. Identity theft can also result from rudimentary tactics with criminals stealing mail, digging through dumpsters, and listening in on phone conversations in public places.

The ultimate goal with many cyber attacks is to steal enough information about a victim to assume their identity to commit fraudulent activity. Unfortunately, most people only discover they're victims of identity theft when they apply for a loan, attempt to open a bank account, apply for a job, receive a call from a collection agency, or request a new credit card.

Cyber criminals prey on corporations, schools, government agencies, hospitals, and other institutions that hold employees' personal information. Because of this, the damage done by identity theft is far-reaching. Cyber criminals hope an employee with access to personal information clicks a link in a phishing email, opening up access to databases of personal and financial information.

Damage done by identity theft has a trickle-down effect, causing personal and emotional trauma for the person who accidentally gives the cyber criminal access to data. There are also severe consequences to the people whose personal information is stolen and the violated organization's reputation.

How Serious Is Identity Theft?

Identity theft is a worldwide threat. Many governments have programs in place to help their citizens report identity theft and establish a recovery plan:

1. In Canada, contact the Canadian Anti-Fraud Call Centre at 1-888-495-8501.
2. In the United States, contact the Federal Trade Commission at 1-877-438-4338.
3. In other counties, check your government's website for information.

A recent IBM report reveals that, on average, a data breach resulting in identity theft costs the violated organization $3.86 million. It typically takes 280 days to realize a data breach has happened.

Social Engineering, Cyber Attacks, and Identity Theft

Identity theft does not happen by accident. Cyber criminals use strategic cyber attack tactics relying on social engineering to trick victims into divulging confidential information they know should not be shared with strangers.

Social engineering relies on the basic human instincts of trust, greed, curiosity, and the desire to convince people to divulge personal and confidential information.

This chain of events often starts with one strategically written phishing email. It convinces a victim to click a link to update their password, giving the cyber criminal access to a corporate database and the personal information of employees, clients, investors, third parties, etc.

How Does Identity Theft Happen?

1 Social engineering with an email, text, or phone message. All it takes is one downloaded file or clicked link in an email or text message to open a gateway to sensitive information.

2 Malware such as installing spyware or keyloggers on the network. Criminals use spyware and key loggers to track your keyboard and online activity to capture passwords, usernames, and other sensitive information.

3 Researching social network sites for personal information, email addresses, employee connections, recent conferences, promotions, etc. Cyber criminals use this information to connect and familiarity themselves with their emails, texts, social media messages, or phone messages – convincing victims to respond.

4 Hacking computers and databases through a range of tactics. From fake websites used to steal passwords, attachments that install ransomware, vulnerabilities in systems, or fake wi-fi access points give access to personal information – cyber criminals have a deep range of hacking tactics.

5 Eavesdropping on telephone conversations in public places, the office building's lobby, on the bus, etc. All it takes is overhearing credit card and address details to have enough information to commit identity theft.

6 Retrieving paper documents from mailboxes, recycling bins, or trash cans and using this information to commit identity theft or additional cyber attacks such as spear phishing or business email compromise.

7 Creating fake online profiles convincing employees who do their due diligence on an unknown caller or email sender that the person is legitimate and can be trusted.

Identity Theft Facts You Need To Know

In 2019, 14.4 million or 1 in 15 people were victims of identity fraud.

1 in 5 identity theft victims experiences identity theft more than once.

Victims lost more than $1.9 billion to identity theft in 2019.

3% of identity theft victims experience emotional distress.

Sources:

Facts + Statistics: Identity theft and cybercrime

The non-economic impacts of identity theft

How Do Cyber Criminals Use Stolen Identities?

Cyber criminals use stolen identities to:

- Accumulate credit card charges on the victim's card.
- Get a new loan or line of credit in the victim's name.
- Transfer funds out of the victim's account without the victim noticing.
- Sign a lease in the victim's name.
- Collect government benefits owed to the victim.
- Submit fraudulent insurance claims in the victim's name.
- Obtain identification or travel documents.
- Apply for jobs, university/college, or grants and bursaries.
- Change usernames and passwords, locking the victim out of their accounts.
- Send phishing, vishing, or smishing attacks to people known to the identity theft victim.
- Hide criminal activities behind the victim's name.

5 Signs Of Identity Theft

Know these five signs of identity theft:

1. Delayed arrival of bills and financial statements. This kind of delay may indicate cyber criminals have changed the mailing address for your accounts or are stealing from your mailbox.
2. Unexpected calls from creditors about outstanding charges and balances on existing accounts or for accounts and charges you did not make.
3. New account confirmation from a bank, credit card company, or online business you are not associated with.
4. Credit card charges and bank account transactions that you did not make.
5. Cancellation notices of utilities or services.

Remember:
Cyber criminals know no bounds with what they will do with your stolen identity. Always verify bank, credit card, and utility statements for unusual charges and activity.

What To Do If You're a Victim of Identity Theft

Number one – do not panic. Cyber criminals are looking for signs you're panicking and may contact you pretending to be an agency who can help you recover from identity theft.

If you're a victim of identity theft:

1. In Canada, contact the Canadian Anti-Fraud Call Centre at 1-888-495-8501.
2. In the United States, contact the Federal Trade Commission at 1-877-438-4338.
3. In other counties, check your government's website for information.