Internet Safety

How to protect yourself Against Cybercrime and Theft and Financial Fraud in the Digital Age

Key Elements

1. Introduction to Internet Safety
2. Identify Cybercrimes and Theft and Financial Fraud
3. Types of Cybercrimes and Theft and Financial Fraud
4. Solutions proposed to protect yourself against Cybercrimes and Theft and Financial Fraud
5. Anti-Cybercrimes Law and Legal Penalties in Saudi Arabia
6. Conclusion
7. References

Introduction to Internet Safety

things we can do online are limitless. The Internet makes it possible to access information quickly, communicate around the world, and much more. Unfortunately, the Internet is also home to certain **risks**, such as **malware**, **spam**, and **phishing**. If you want to stay safe online, you'll need to understand these risks and learn how to avoid them.

In simple terms, **online safety** refers to the act of staying **safe online**. ... Being **safe online means** individuals are protecting themselves and others from **online** harms and risks which may jeopardise their personal information, lead to unsafe communications or even effect their mental health and wellbeing.

Identify Cybercrimes & Theft & Financial Fraud?

Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device. Most, but not all, **cybercrime** is committed by **cybercriminals** or hackers who want to make money.

Financial fraud happens when someone deprives you of your money or otherwise harms your **financial** health through misleading, deceptive, or other illegal practices. This can be done through a variety of methods such as identity theft or investment **fraud**.

Fraud and financial crimes are a form of **theft**/larceny that occur when a person or entity takes money or property, or uses them in an illicit manner, with the intent to gain a benefit from it.

The basic **difference between theft** and **fraud** is that **theft** generally involves taking something through force or by stealth, where **fraud** revolves around a purposeful misrepresentation of fact, and the basic **difference between** criminal **fraud** and civil **fraud** lies in who is pursuing legal action **in the** case.

Types of Cybercrimes & Theft & Financial Fraud

Cybercrime Types:

- Email and internet fraud.
- Identity fraud (where personal information is stolen and used).
- Theft of financial or card payment data.
- Theft and sale of corporate data.
- Cyberextortion (demanding money to prevent a threatened attack).

- Ransomware attacks (a type of cyberextortion).
- Cryptojacking (where hackers mine cryptocurrency using resources they do not own).
- Cyberespionage (where hackers access government or company data).
- Most cybercrime falls under two main categories:
- Criminal activity that *targets*
- Criminal activity that *uses* computers to commit other crimes.

Online Theft Types:

- Account Takeover Fraud.
- Debit Card Fraud or Credit Card Fraud.
- Driver's License Identity Theft.
- Mail Identity Theft.
- Online Shopping Fraud.
- Social Security Number Identity Theft.
- Senior Identity Theft and Scams.
- Child Identity Theft.

Types of Financial Frauds:

- Mail Fraud.
- Driver's License Fraud.
- Healthcare Fraud.
- Debit and Credit Card Fraud.
- Bank Account Takeover Fraud.
- Stolen Tax Refund Fraud.
- Voter Fraud.
- Internet Fraud.
- Elder Fraud.

Solutions Proposed to Protect Yourself Against Cybercrimes & Theft & Financial Fraud

1. Use a full-service internet security suite

For instance, Norton Security provides real-time protection against existing and emerging malware including ransomware and viruses, and helps protect your private and financial information when you go online.

2. Use strong passwords

Don't repeat your passwords on different sites, and change your passwords regularly. Make them complex. That means using a combination of at least 10 letters, numbers, and symbols. A password management application can help you to keep your passwords locked down.

3. Keep your software updated

This is especially important with your operating systems and internet security software. Cybercriminals frequently use known exploits, or flaws, in your software to gain access to your system. Patching those exploits and flaws can make it less likely that you'll become a cybercrime target.

4. Manage your social media settings

Keep your personal and private information locked down. Social engineering cybercriminals can often get your personal information with just a few data points, so the less you share publicly, the better. For instance, if you post your pet's name or reveal your mother's maiden name, you might expose the answers to two common security questions.

5. Strengthen your home network

It's a good idea to start with a strong encryption password as well as a virtual private network. A VPN will encrypt all traffic leaving your devices until it arrives at its destination. If cybercriminals do manage to hack your communication line, they won't intercept anything but encrypted data. It's a good idea to use a VPN whenever you a public Wi-Fi network, whether it's in a library, café, hotel, or airport.

6. Talk to your children about the internet

You can teach your kids about acceptable use of the internet without shutting down communication channels. Make sure they know that they can come to you if they're experiencing any kind of online harassment, stalking, or bullying.

7. Keep up to date on major security breaches

If you do business with a merchant or have an account on a website that's been impacted by a security breach, find out what information the hackers accessed and change your password immediately.

8. Take measures to help protect yourself against identity theft

Identity theft occurs when someone wrongfully obtains your personal data in a way that involves fraud or deception, typically for economic gain. How? You might be tricked into giving personal information over the internet, for instance, or a thief might steal your mail to access account information. That's why it's important to guard your personal

data. A VPN — short for virtual private network — can also help to protect the data you send and receive online, especially when accessing the internet on public Wi-Fi.

9. Know that identity theft can happen anywhere

It's smart to know how to protect your identity even when traveling. There are a lot of things you can do to help keep criminals from getting your private information on the road. These include keeping your travel plans off social media and being using a VPN when accessing the internet over your hotel's Wi-Fi network.

10. Keep an eye on the kids

Just like you'll want to talk to your kids about the internet, you'll also want to help protect them against identity theft. Identity thieves often target children because their Social Security number and credit histories frequently represent a clean slate. You can help guard against identity theft by being careful when sharing your child's personal information. It's also smart to know what to look for that might suggest your child's identity has been compromised.

11. Know what to do if you become a victim

If you believe that you've become a victim of a cybercrime, you need to alert the local police and, in some cases, the FBI and the Federal Trade Commission. This is important even if the crime seems minor. Your report may assist authorities in their investigations or may help to thwart criminals from taking advantage of other people in the future. If you think cybercriminals have stolen your identity. These are among the steps you should consider.

- Contact the companies and banks where you know fraud occurred.
- Place fraud alerts and get your credit reports.
- Report identity theft to the FTC.

Anti-cybercrimes Law
&
Legal Penalties in Saudi Arabia

A penalty of imprisonment for a period not exceeding a year and a fine not exceeding five hundred thousand riyals, or either of these two punishments; Every person who commits any of the following information crimes:

1 - Tapping, capturing, or intercepting what is sent via the information network or a computer device - without a valid legal justification.

2 - Unlawful entry to threaten or extort a person; To compel him to perform or abstain from an action, even if doing or abstaining from this act is legitimate.

3 - Unlawful access to a website, or entry to a website to change the designs of this website, destroy it, modify it, or occupy its address.

4- Infringement of private life through misuse of camera mobile phones, or the like.

5- Defaming others and harming them, through the means of various information technology.

Punished by imprisonment for a period not exceeding four years and a fine not exceeding three million riyals, or one of these two punishments; Every person who commits any of the following information crimes:

1- Unlawful entry to delete private data, delete it, destroy it, leak it, destroy it, change it, or re-publish it.

2 - Stopping the information network from working, disrupting it, or destroying, or erasing, programs or data existing or used in it, deleting it, leaking it, destroying it, or modifying it.

3- Obstructing access to the service, or disrupting it, or disrupting it, by any means.

Every person who commits any of the following information crimes shall be punished by imprisonment for a period not exceeding ten years and a fine not exceeding five million riyals, or by one of these two penalties:

1- Establishing or publishing a website for terrorist organizations on the information network or a computer device; To facilitate contact with the leaders of these organizations, or any of their members, or to promote or fund their ideas, or to publish how to manufacture incendiary devices, explosives, or any tool used in terrorist acts.

2 - Illegal access to a website or an information system directly, or through an information network, or a computer device, to obtain data affecting the internal or external security of the state, or its national economy.

Conclusion

In Conclusion, one’s privacy on the internet is very important because of all the applications, services, scams and viruses on the internet that are waiting for any given chance to steal someone's personal material. If all people could protect themselves and use the right software, they would be much safer, and it would be harder to have personal information stolen from them. Anyone using the internet should take into consideration this information will help them in the future to protect their privacy and maintain security.

References

1. https://edu.gcfglobal.org/en/internetsafety/introduction-to-internet-safety/1/
2. https://www.kaspersky.com/resource-center/threats/what-is-cybercrime
3. https://us.norton.com/internetsecurity-how-to-how-to-recognize-and-protect-yourself-from-cybercrime.html
4. https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/25df73d6-0f49-4dc5-b010-a9a700f2ec1d/1