Online Identity Theft

Target Group
People with Special Needs

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

Online Identity Theft

Target Group: People with Special Needs

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

Intellectual Property Rights

January 2025
Doha, Qatar

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

To contact the National Cyber Security Academy

00974 404 663 79
00974 404 663 62
www.ncsa.gov.qa/
academy@ncsa.gov.qa

Dear Participant,

In the era of rapid technological advancement and the internet being part of our daily lives, cyber threats have become an ever-present concern for all segments of society. It is imperative that we raise awareness about digital safety concepts, which serve as a protective shield against these threats.

The National Cyber Security Agency, in its commitment to enhance digital safety indicators within the community as part of the "National Initiative for Digital Safety", has developed this booklet. It aims to provide a comprehensive guide, offering general advice and guidelines related to digital safety.

Table of Contents	Page

Introduction

Online identity theft is one of the most prominent cybercrimes increasing with technological development and individuals' growing reliance on the internet in their daily lives. This type of crime doesn't target a specific group but can affect anyone, regardless of age or technical expertise. Criminals involved in this type of fraud rely on social engineering techniques, which are advanced tools used to deceive individuals through psychological manipulation. By provoking feelings of fear or urgency in their victims, they prompt them to make hasty decisions, such as providing personal or financial information without sufficient consideration.

Additionally, Criminals also impersonate trusted entities, such as banks, financial institutions, or even government agencies, to lead victims to believe they are interacting with a legitimate organisation. These criminals use multiple methods to reach their victims, including sending fake emails, using fake websites that appear like original ones, or even making convincing phone calls. Once they manage to deceive victims into obtaining their personal data, such as passwords or bank account numbers, they can exploit this information to carry out illegal financial operations, identity theft, or access private accounts.

Identity theft extends beyond the mere theft of personal information; it can also lead to turning compromised devices into tools for attacking other people or companies. In some cases, infected computers or phones are used to execute wider attacks such as Denial of Service (DDoS) attacks, by directing several fake requests toward a specific website to disable it. These attacks highlight the complexity of cyber threats in the current era and the fact that online identity theft can be an introduction to a series of other crimes that threaten digital security on a wide scale.

With individuals and companies increasingly relying on the internet to manage their financial and personal affairs, protecting digital identity has become more essential than ever. Therefore, users should be aware of the dangers of identity theft and how to prevent it, in addition to adopting advanced protection techniques such as encryption and multi-factor authentication to maintain cybersecurity.

01

Chapter One

The Concept of Identity Theft

- First: **Identity Theft Attacks and Their Types**
- Second: **Causes of Online Identity Theft**
- Third: **Impacts of Identity Theft**

The Concept of Identity Theft

Identity theft is considered one of the most dangerous electronic crimes threatening individuals and companies in today's digital world. The term "identity theft" refers to the illegal acquisition of someone's personal information, such as name, ID number, bank accounts, or credit card details, for fraudulent purposes. "Identity forgery" is the process of using this information to impersonate another person or claim a fake identity to deceive victims or institutions for financial or social gains.

With the rapid development of technology and increased reliance on the internet for personal and financial transactions, it has become easier for cybercriminals to access and exploit sensitive information. This often happens through advanced techniques such as social engineering, phishing, or hacking online accounts. In other cases, criminals may target data through malicious software that collects personal information from compromised devices.

The consequences of identity theft are not limited to financial damages but can also lead to serious legal and social implications. It can be used to commit other crimes such as opening fake bank accounts, applying for loans, or even executing fraud using the victim's name.

Countering these crimes has become a major challenge for governments and security institutions. Protection from identity theft and impersonation requires multi-factor efforts, including awareness of best digital safety practices, implementing advanced encryption techniques and developing strict laws that criminalize these activities and deter criminals.

First: Identity Theft Attacks and Their Types

An identity theft attack is a type of phishing attack where internet criminals pretend to be real people or legitimate entities to steal sensitive personal data from individuals and employees working in institutions through social engineering tactics. They try to deceive the victim into transferring money, providing sensitive information, or providing login credentials for banking and digital accounts, and other unauthorized critical information[1].

An example of a successful impersonation attack is when criminals use a spoofed email of a senior executive or important business entity, a tactic known as Business Email Compromise (BEC). The criminal deceives their victims into making a financial transfer or providing important information that helps them gain unauthorised access to systems and networks. The theft may be an initial and preparatory step for another cybercrime, such as installing malware on the victim's devices to steal sensitive data and threaten the victim, or to be their gateway to access connected devices on the same network and systems, especially in workplaces.

Did you know?

One in every 3,226 emails sent approximately once a month received by a senior employee is an identity theft attempt or phishing[2].

1. What is Impersonation in Cybersecurity? Zero Fox, available at: https://www.zerofox.com/glossary/impersonation-in-cybersecurity/
2. Kyle Chin, What is an Impersonation Attack?, September 2024. available at: https://www.upguard.com/blog/impersonation-attack#:~:text=An%20impersonation%20attack%20is%20a%20type%20of%20targeted%20phishing%20attack

Types of Identity Theft Attacks

Cybercriminals try to impersonate someone in different ways using phishing methods. There are several types of identity theft attacks:

Email Impersonation Attacks

One way to carry out identity theft attacks for cybercriminals is to pretend to be colleagues or executive managers using a fake or stolen email account. Identity theft or direct phishing attacks are considered highly advanced and targeted attacks, unlike mass phishing attacks via email that end up in the spam folder.

Email identity theft attacks often contain harmful links or attachments that direct users to malicious websites once clicked. Other attacks, such as social engineering, are used to deceive the victim and convince them to reveal critical data or transfer money directly to the criminal[(1)].

1. Email Impersonation Attacks, Proof Point, available at: https://www.proofpoint.com/us/threat-reference/impersonation-attack

Common signs of email identity theft attacks include:

- Urgent requests involving pressure to transfer funds or disclose sensitive information such as bank account details or login credentials.
- Employees requesting sudden changes to direct deposit information.
- Spelling and grammatical errors in emails, such as writing the letter “m” as “rn.”
- Language that evokes feelings of urgency, fear and tension.
- The fake email is usually a slightly modified version of the original email address, and the actual URLs within the email don’t match the text in the hyperlinks in the email copy(1).

1. Impersonation Attack. follow link: https://www.mimecast.com/content/impersonation-attack/

Second: Causes of Online Identity Theft

Identity theft is one of the most widespread cybercrimes, causing serious damage to individuals and companies. Forms of identity theft vary from stealing financial information to impersonation on social media. Among the most prominent causes of online identity theft:

Excessive Use of Internet and Digital Communication

One of the main reasons behind the increase in identity theft cases is the extensive use of the internet. With most life activities shifting to the digital world, from online shopping to banking transactions, it has become easy for criminals to exploit this open environment to access personal information.

Many people's daily lives have become significantly tied to the internet, with individuals relying on digital applications and platforms for communication, shopping and financial transactions. With this heavy reliance, opportunities have increased for internet criminals to exploit any vulnerability to access sensitive data, whether financial or personal. Additionally, many individuals conduct online transactions without verifying the security of websites or applications they use, allowing attackers to exploit these unsecured transactions to obtain sensitive information such as credit card numbers or login credentials.

Lack of Awareness about Digital Safety Basics Among Users

Digital safety awareness is the first line of defence against cybercrimes. Unfortunately, many users experience a deficiency in understanding the essential protective measures, making them vulnerable to hacking and data theft. Several users rely on weak and easily predictable passwords such as “123456” or “password”. This habit makes it easy for attackers to execute password-guessing attacks or use hacking programmes to access accounts.

Did you know?

80% of electronic breaches occur due to using weak passwords or reusing them across multiple accounts[1].

1. Stouffer, Clare. 139 password statistics to help you stay safe in 2024 Norton, june 2023, available at: https://us.norton.com/blog/privacy/password-statistics

Increase in Security Vulnerabilities in Systems and Applications

As systems and applications become more complex, the possibility of security vulnerabilities increases. New vulnerabilities are continuously discovered, and software developers work on addressing them through regular updates. However, users' failure to install these updates may lead to successful cybercrimes. At the same time, hacking techniques constantly evolve with technology development. Methods such as phishing, malware attacks and spyware have become more advanced, enhancing cybercriminals' chances of successfully targeting individuals and companies. Among the most attractive targets for these criminals are online banking and financial applications. Vulnerabilities in these applications pose a significant threat, as attackers can exploit these weaknesses to gain access to users' accounts and easily steal their funds or financial information.

Phishing Attacks and Malware Proliferation

Phishing is one of the most common methods of identity theft, where attackers rely on sending emails or text messages that appear to be from trusted entities such as banks or major corporations. Their goal is to deceive users into revealing sensitive information. These fraudulent messages often contain links that lead users to fictitious websites carefully designed to mimic the official websites of the claimed sender. If users enter their personal information on these sites, this information is directly transmitted to the attackers.

In addition to phishing, malware plays a significant role in hacking attacks. These malicious software are among the most dangerous tools attackers use to breach devices and steal data. They include spyware capable of monitoring all user activities on their device, including recording passwords and personal information, which increases the risk of identity theft and privacy violations[1].

Did you know?

Around 20% of users encounter phishing attempts annually.

1. Kinza. Yasar, What is malware? Prevention, detection and how attacks work, Tech Target, july 2024, available at: https://www.techtarget.com/searchsecurity/definition/malware

Public Wi-Fi Networks

Many users rely on public wireless networks in places like cafes or airports. However, these networks are often insufficiently secured, making them ideal environments for criminals to exploit connected devices. When connecting to an unsecured wireless network, it becomes easy for attackers to monitor data traffic between the device and the network. If this data is unencrypted, they can access sensitive information such as passwords, credit card numbers and any other data transmitted over the internet.

To counter these risks, using a Virtual Private Network (VPN) is one of the efficient ways to protect data when connecting to unsecured networks. VPNs encrypt data traffic between the device and the network, making it difficult for attackers to spy on or access it, thus providing an additional layer of security for users in such environments[1].

1. What is a VPN service?, Microsoft. Available at: https://azure.microsoft.com/en-ca/resources/cloud-computing-dictionary/what-is-vpn

Psychological and Social Exploitation (Social Engineering)

Social engineering is a type of fraud that primarily relies on exploiting human nature and deceiving individuals into providing sensitive information without realising the danger. Attackers in this method base their approach on studying victim behaviours and psychological aspects to convince them to reveal their personal data. One of their most prominent methods is identity impersonation, where criminals pretend to be trusted figures such as bank employees or company officials, using this status to convince individuals to reveal their information. This method exploits trust and social relationships to bypass any technical security barriers that may exist.

Moreover, attackers resort to provoking fear or suggesting the existence of emergencies, compelling victims to act swiftly without thinking. A person might receive a phone call claiming their bank account is under attack and needs immediate information provision for protection. Under the pressure of this emergency, victims make hasty decisions, facilitating access to personal data for attackers.

Facts and Information

Social engineering is responsible for 30% of successful cyberattacks globally.

Third: Impacts of Identity Theft

Identity theft is a crime with serious consequences that extend beyond mere loss of personal information. The impacts of identity theft encompass financial, psychological and legal aspects, causing long-term damage to individuals and companies.

Financial Damages

Financial damages are among the primary direct consequences of identity theft. Criminals exploit stolen financial information, such as bank account details or credit cards, for illegal gains. These damages manifest in various forms, but the most common is the direct theft of money from victims' accounts. When criminals gain access to account information, they can withdraw funds or make unauthorised financial transfers, causing sudden decreases in bank balances or theft of large amounts without warning. It is often difficult to recover these funds promptly, and in some cases, it may be impossible.

Besides direct theft of money, victims face the risk of accumulating debt due to criminals using their identity to open new accounts or apply for loans or credit cards. These debts, of which the victims are completely unaware, can lead to serious financial problems. Victims may find themselves required to repay loans they did not take out or burdened by debts that have accumulated without their involvement. These consequences can persist for long periods, as legal and financial procedures take time to resolve, affecting victims' credit records and exposing them to long-term financial difficulties.

Psychological Effects

The impacts of identity theft are not limited to financial damages alone; they extend to include profound and long-lasting psychological effects on victims. Dealing with the consequences of this crime can be mentally exhausting, leaving a permanent impact on the mental health of those affected.

One of the main effects is constant anxiety, where victims suffer from persistent fear about the safety of their personal and banking information. This anxiety remains even after discovering the theft, as fear of incident recurrence or the possibility of additional information falling into criminals' hands remains a source of continuous stress. Victims also feel unable to protect their digital privacy, increasing feelings of tension and suspicion in all their future transactions.

Furthermore, victims suffer from a sense of loss of control, facing feelings of helplessness regarding control over their personal information. Realising that someone can use their identity or financial information without permission makes victims feel a loss of authority over aspects of their lives. This sense of helplessness can escalate to lead to feelings of frustration and despair, negatively affecting victims' daily lives.

In some cases, the psychological stress resulting from identity theft can lead to depression and social isolation. Victims feel targeted and vulnerable, leading them to avoid digital and banking activities that might expose them to theft again. They become more isolated, withdrawing from social life or dealing with technology in general, deepening their feelings of sadness and despair.

Impacts on Work and Professional Life

The impact of Identity theft is not limited to financial or psychological aspects but extends significantly to impact victims' professional lives. When an individual's identity is used in illegal or fraudulent activities, it can damage their reputation in the workplace, leading to severe consequences for their career.

One of the main impacts of identity theft is the loss of job opportunities. Victims may face difficulty in employment if their personal information becomes associated with legal issues that affect their professional reputation. In certain cases, they may be dismissed when hiring managers discover their record of suspicious activities. This can be frustrating for victims as they are deemed unqualified due to actions they did not commit.

Moreover, the negative impacts on future employment pose another challenge for victims, as identity theft may lead to the deterioration of their credit and legal records. This makes it challenging to obtain future employment opportunities that require a criminal record or credit check. In many industries, these checks are essential for the hiring process. Consequently, having negative information in one's record may result in losing important job opportunities.

This situation complicates victims' ability to build a stable career path, as they find themselves caught between the repercussions of identity theft and its resulting legal and social consequences. Under these circumstances, significant effort is required to overcome these challenges and rebuild their professional reputation, making it necessary to enhance awareness about the importance of protecting personal identity and how to counter such crimes.

02

Chapter 2

Protection Methods and Post-Identity Theft Procedures

- First: **Methods of Protection Against Identity Theft**
- Second: **Post-Identity Theft Procedures**

Protection Methods and Post-Identity Theft Procedures

Identity theft is one of the most serious cybercrimes threatening individuals and organisations, as it can lead to substantial financial, psychological and legal repercussions. Consequently, it is essential to adopt proactive measures to reduce the risk of becoming a victim of this type of crime. These measures include maintaining the confidentiality of personal information, using strong and diverse passwords, and enabling two-factor authentication for sensitive accounts. Additionally, individuals must ensure regular updates of protection software and share personal data online only with trusted entities.

First: Protection Methods Against Identity Theft

Identity theft represents one of the most prominent threats in the digital age. With increasing reliance on the internet for financial and personal transactions, preserving one's digital identity has become an urgent necessity, as unauthorised access to personal data can cause severe financial and psychological damage. Fortunately, some steps can be taken to enhance digital safety indicators and reduce the risk of identity theft:

Using Strong and Complex Passwords

Passwords are the first line of defense against identity theft attempts, making it essential to prioritize their security. Weak or repetitive passwords significantly increase the possibility of account breaches(1).

Strong Password Requirements

The ideal password should contain a diverse combination of uppercase and lowercase letters, numbers and special characters. The more complex the password, the harder it is for hackers to breach it. It is preferred that the password contain at least 12 characters to reduce the possibility of exposure using random encryption tools.

Avoiding Password Repetition

Using the same password for multiple accounts is a common mistake. If one account is breached, the hacker may gain access to other accounts using the same password. Therefore, it is recommended to create unique passwords for each account or service.

Using Password Management Tools

To avoid the issue of forgetting complex passwords, users can use password management software, which securely stores passwords and allows users to create unique, complex passwords for each account. These tools provide protection by encrypting data and adding an additional layer of security.

1. What Is Password Protection?, Proof Point, available at: https://www.proofpoint.com/au/threat-reference/password-protection

Did you know?

Studies have found that 81% of data breaches are due to using weak or reused passwords[1].

Enabling Two-Factor Authentication

One of the effective means to enhance account security is activating two-factor authentication, a security system that adds a layer of protection alongside the password. Even if a hacker discovers the password, this feature requires another step to verify the user's identity.

Two-factor verification requires adding a second verification step, such as sending a temporary code to a mobile phone or email. Therefore, even if the password is breached, the attacker cannot access the account without access to the other device used for verification.

1. Rob Sobers, Must-Know Data Breach Statistics, Varoni, September 2024, available at: https://www.varonis.com/blog/data-breach-statistics

Types of Two-Factor Authentication

Two-factor authentication methods include:

- **SMS:** Sending a temporary code to the user's phone number.
- **Dedicated Applications:** Such as Google Authenticator or Authy, which generate temporary authentication codes.
- **Biometric Authentication:** Such as fingerprint or facial recognition to confirm identity.

Activating two-factor authentication significantly hinders hackers' ability to access accounts by providing an extra layer of security. Additionally, numerous banking services, social networks and email providers offer this feature, and it is advisable to enable it on all applicable accounts[1].

Did you know?

Adding two-factor authentication can reduce the possibility of account breaches by up to 99%.

1. Biometric Verification, Login TC, available at: https://www.loginTC.com/types-of-authentication/biometric-authentication

Updating Software and Security Systems

Software and security system updates are among the most necessary preventive measures for protecting digital identity and maintaining the security of devices and personal information. These updates often contain fixes for security vulnerabilities that attackers could exploit to breach systems and steal data.

The importance of updating software lies in addressing vulnerabilities that may be discovered over time. Outdated software, particularly those which are not updated for extended periods, often contains flaws that make it susceptible to cyberattacks. Developers regularly release updates to patch these security gaps. If a user neglects to update their software and systems, they remain vulnerable to attacks that could be exploited by hackers, thereby increasing the risk of identity theft or the compromise of sensitive information.

Regarding operating system updates, such as Windows and macOS, they are essential to ensure protection against the latest cyber threats. It is recommended to enable automatic updates so that security updates are installed immediately without requiring user intervention, thus enhancing system protection against evolving threats.

In addition to operating systems, applications and security tools should be updated regularly. Applications dealing with sensitive data, such as banking and e-commerce applications, require continuous updating to ensure potential security vulnerabilities are addressed. Antivirus software and firewalls also need periodic updates to remain capable of detecting and combating the latest threats and malware[1] .

In conclusion, regular software updates are among the most crucial preventive measures for safeguarding digital identity and protecting it from rising threats.

Did you know?

Studies indicate that 60% of breach incidents result from the exploitation of vulnerabilities in software that has not been properly updated.

1. Application Security Tools - How and when to use them, jit, available at: https://www.jit.io/resources/appsec-tools

Avoiding Unsafe Sharing of Personal Information

Sharing personal information online is one of the main factors leading to identity theft. In the age of digital expansion, users must carefully handle any request for sensitive information and ensure that the entity or website requesting this information is trusted and secure to ensure data protection from breaches.

Verifying secure websites is a fundamental step when providing personal information online. It is necessary to ensure the site uses HTTPS protocol instead of HTTP, as HTTPS provides an encrypted connection between the user and the website, reducing the possibility of hackers intercepting data. This protocol can be verified by looking for the lock icon in the address bar next to the website address[1] .

Moreover, avoiding sharing sensitive information through unsecured messages is crucial. Information such as bank account numbers or passwords should not be shared via text messages or regular email as they are easily susceptible to breaches. Use secure and encrypted means such as encrypted messaging applications to reduce leak risks when necessary.

1. Use HTTPS across your website, available at: https://www.ownyouronline.govt.nz/business/get-protected/guides/benefits-of-using-https-across-your-website

Using Encryption Techniques

Encryption is one of the most effective measures for protecting personal data and sensitive information during transmission over the internet. This technique involves converting data into an unintelligible format, rendering it useless to any unauthorised party attempting to access it. Even if hackers manage to intercept encrypted data, they will face significant challenges in decrypting and interpreting it[1].

Amidst the growing threats of cyberattacks, encryption has become an essential tool for ensuring data security. For instance, when sending emails containing sensitive information or storing important documents on a computer, it is strongly recommended to employ appropriate encryption techniques to protect such data from unauthorised access.

Furthermore, numerous digital platforms adopt encryption systems to ensure the security of communications and information. For example, email services offer encryption options for messages, ensuring their content remains inaccessible except to the intended recipients. Similarly, modern messaging applications implement end-to-end encryption, ensuring that messages remain encrypted from the moment they are sent until they are received.

Encryption serves as the cornerstone of modern digital security strategies, providing robust protection against cyberattacks and safeguarding data privacy in an increasingly technology-dependent world.

1. Zoran Cocoara, Data Encryption: Protecting Sensitive Information in the Digital Age, End Point Protector, November 2023, available at:https://www.endpointprotector.com/blog/data-encryption-protecting-sensitive-information

Second: Post-Identity Theft Procedures

Identity theft can be a devastating experience that affects financial and personal aspects. When an individual falls victim to identity theft, it is crucial to take prompt action to protect personal information and reduce potential damages. Therefore, several steps can be taken in the event of identity theft:

1 Reporting the Crime

The first step to take upon discovering identity theft is to report the crime to the Cyber Crime Combating Department at the Ministry of Interior. Prompt reporting can help prevent the situation from worsening and protect the victim from further harm.

2 Notifying Financial Institutions

After reporting the incident, it is essential to immediately contact the banks and financial institutions managing the affected accounts. Early notification can help protect these accounts from any unauthorised transactions. The victim should also request the freezing or closure of the impacted accounts to prevent any unlawful use.

3 Notifying Credit Bureaus

Additionally, it is important to inform credit bureaus, as they can place a fraud alert on your credit report. This means that any institution attempting to open a new account in your name will be notified that you are a victim of identity theft. This action helps to reduce the chances of your personal information being exploited in the future.

4 Credit Freeze

Credit freezing is essential to prevent attackers from opening new accounts or conducting transactions in your name using stolen information. This procedure prevents anyone else from accessing your credit report without your consent, making it difficult for criminals to benefit from your stolen identity.

Warning!

Be cautious of sharing information on public networks; connecting to unsecured public Wi-Fi networks exposes your data to theft. Use a Virtual Private Network (VPN) to protect your data while browsing the internet in public places[1].

5 Credit Monitoring

After reporting the crime and freezing your credit, it is essential to monitor your credit to ensure there are no unauthorised activities linked to your personal information. By monitoring your accounts and credit reports, you can promptly identify suspicious activities and take the necessary actions quickly.

6 Self-Monitoring

You can also regularly monitor your credit report by obtaining a copy from major credit bureaus. In some countries, consumers are entitled to a free credit report once a year. By reviewing the report regularly, you can detect any unfamiliar activities and respond accordingly.

7 Early Warnings

Credit monitoring helps to detect crimes early before they escalate. If you observe any unusual activity, such as a significant increase in your balance due or the opening of new accounts without your permission, you should promptly report these incidents to the relevant banks and take appropriate measures.

1. Andra Zaharia, The Dangers of Using Public Wi-Fi, Aura , January 2023, available at: https://www.aura.com/learn/dangers-of-public-wi-fi

Exercises are based on the material presented in this booklet, and are provided here without answers. An answer key is provided at the end of the booklet

First Exercise

Mark the following statements as (True) or (False), and correct any errors if found

1. Identity theft occurs when using another person's data for legal purposes.
2. Using strong and complex passwords can reduce the possibility of identity theft.
3. Connecting to public Wi-Fi networks poses no risk to identity theft.
4. Phishing is a method used by fraudsters to obtain personal data by impersonating trusted entities.

5. Password management software can securely store and encrypt passwords.

6. Cybercriminals primarily rely on technical vulnerabilities and do not exploit victims' psychological aspects.

7. Using the same password for all accounts enhances security.

8. Encryption is not an effective means of protecting data during internet transmission.

Second Exercise

• Choose the correct answer

1. What is one method of protecting digital identity?

1 Using the same password for each account.

2 Using complex passwords.

3 Not updating software.

2. Which of the following is an example of phishing?

1 An email from a friend.

2 An email appearing to be from a bank requesting financial information.

3 Visiting a government website.

3. What is the primary goal of identity theft?

1. Obtaining financial data.
2. Learning personal information only.
3. Opening legal accounts.

4. What is the safest way to use public Wi-Fi network?

1. Connecting directly to the network.
2. Using a VPN.
3. Never using the network at all.

5. What security protocol should be verified when using a website?

1. HTTP
2. HTTPS
3. FTP

6. What helps prevent identity theft?

1. Not monitoring financial accounts.
2. Regular monitoring of credit accounts.
3. Continuously opening new accounts.

7. Which of the following describes "social engineering"?

1. Hacking a banking system.
2. Convincing victims to provide their personal information.
3. Updating security systems.

Third Exercise

Complete the following sentences

1. Two-factor authentication adds an additional ..... for protection of accounts from identity theft.
2. Using ..... helps protect data when connecting to public Wi-Fi networks.
3. ..... is one of the key means of protection against online identity theft.
4. Avoid using ..... in several accounts to reduce the risk of hacking.
5. When receiving an email requesting personal information, one must verify the ..... to ensure its authenticity.
6. Phishing occurs through sending ..... that appear to be from trusted entities to deceive the victim.
7. Password management software store passwords and ..... encrypt them.
8. Software updates help patch security .....

Answer Key

Question

First Exercise Answers: Mark the following statements as (True) or (False), and correct any errors if found

Answer

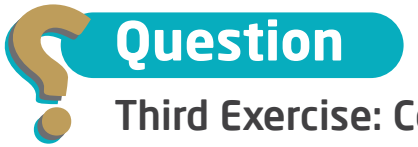
1. **False:** Identity theft occurs for fraudulent or illegal purposes.
2. **True**
3. **False:** Connecting to public Wi-Fi networks exposes data to theft unless using a VPN.
4. **True**
5. **True**
6. **False:** They also rely on social engineering and exploit trust and fear.
7. **False:** Using one password exposes all accounts to risk if one is compromised.
8. **False:** Encryption is one of the most effective means of data protection.

Question

Second Exercise Answers: Choose the correct answer

Answer

1. What is one method of protecting digital identity?
   Answer: Using complex passwords.
2. Which of the following is an example of phishing?
   Answer: An email appearing to be from a bank requesting financial information.
3. What is the primary goal of identity theft?
   Answer: Obtaining financial data.
4. What is the safest way to use public Wi-Fi network?
   Answer: Using a VPN.
5. What security protocol should be verified when using a website?
   Answer: HTTPS
6. What helps prevent identity theft?
   Answer: Regular monitoring of credit accounts.
7. Which of the following describes “social engineering”?
   Answer: Convincing victims to provide their personal information.



Question

Third Exercise: Complete the following statements

Answer

1. Two-factor authentication adds an additional **Security layer** for protection of accounts from identity theft.

2. Using **VPN** helps protect data when connecting to public Wi-Fi networks.

3. **Encryption** is one of the key factors of protection against online identity theft.

4. Avoid using **the same password** in several accounts to reduce the risk of hacking.

5 When receiving an email requesting personal information, one must verify the **source** to ensure its authenticity.

6 Phishing occurs through sending **Email messages** that appear to be from trusted entities to deceive the victim.

7 Password management programmes store passwords and **Automatically** encrypt them.

8 Software updates help patch security **Vulnerabilities** .

References

1. What is Impersonation in Cybersecurity? Zero Fox, available at: https://www.zerofox.com/glossary/impersonation-in-cybersecurity/
2. Kyle Chin, What is an Impersonation Attack?, September 2024. available at: https://www.upguard.com/blog/impersonation-attack#:~:text=An%20impersonation%20attack%20is%20a%20type%20of%20targeted%20phishing%20attack
3. Email Impersonation Attacks, Proof Point, available at: https://www.proofpoint.com/us/threat-reference/impersonation-attack
4. Impersonation Attack. follow link: https://www.mimecast.com/content/impersonation-attack/
5. Stouffer, Clare. 139 password statistics to help you stay safe in 2024 Norton, June 2023, available at: https://us.norton.com/blog/privacy/password-statistics
6. Kinza. Yasar, What is malware? Prevention, detection and how attacks work, Tech Target, July 2024, available at: https://www.techtarget.com/searchsecurity/definition/malware

7. What is a VPN service?, Microsoft. Available at: https://azure.microsoft.com/en-ca/resources/cloud-computing-dictionary/what-is-vpn

8. What Is Password Protection?, Proof Point, available at: https://www.proofpoint.com/au/threat-reference/password-protection

9. Rob Sobers, Must-Know Data Breach Statistics, Varoni, September 2024, available at: https://www.varonis.com/blog/data-breach-statistics

10. Biometric Verification, Login TC, available at: https://www.logintc.com/types-of-authentication/biometric-authentication/

11. Application Security Tools – How and when to use them, jit, available at: https://www.jit.io/resources/appsec-tools

12. Use HTTPS across your website, available at: https://www.ownyouronline.govt.nz/business/get-protected/guides/benefits-of-using-https-across-your-website/

13. Zoran Cocoara, Data Encryption: Protecting Sensitive Information in the Digital Age, End Point Protector, November 2023, available at: https://www.endpointprotector.com/blog/data-encryption-protecting-sensitive-information/

14. Andra Zaharia, The Dangers of Using Public Wi-Fi, Aura , January 2023, available at: https://www.aura.com/learn/dangers-of-public-wi-fi