Cyber Fraud and Forgery

Target Group

Senior Citizens

الأكاديمية الوطنية للأمن السيبراني

National Cyber Security Academy

Cyber Fraud and Forgery

Target group: Senior Citizens

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

Intellectual Property Rights

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

Contact the National Cyber Security Academy

📱 00974 404 663 79 ☎ 00974 404 663 62

🌐 www.ncsa.gov.qa/ ✉ academy@ncsa.gov.qa

January 2025
Doha, Qatar

Dear Participant

With rapid technological progress and the Internet's expansion across all areas of life, cyber threats are now a concern for all segments of society. This highlights the necessity to raise awareness of digital safety principles, serving as a critical shield against these threats.

As part of the National Initiative for Digital Safety aimed at enhancing community-wide digital safety, the National Cyber Security Agency presents this booklet, offering a range of general tips and guidelines on digital safety.

Introduction

In the current digital revolution, numerous new terms related to crime have emerged, especially regarding cybercrimes targeting computers and networks. Cybercrimes exploit technologies to engage in unlawful activities for financial gain or personal motives and are often committed by hackers or cybercriminals.

Cybercrime involves various types, such as email and Cyber fraud, identity theft where personal information is stolen and misused, and financial data theft including credit card information. These crimes, known as ransomware attacks, also include copyright violations and the sale of illegal goods online.

According to Accenture's 2021 Cyber Resilience Report, digital attacks increased by 31% from 2020 to 2022, with annual attacks per company rising from 206 to 270. These attacks also impact individuals, as many companies hold important personal customer information. A single attack, whether a data breach, malware, ransomware, or denial of service, can cost companies an average of $200,000[1].

Did You Know?

Downloading applications from reputable stores reduces the risk of online fraud.

In 2021, Javelin Strategy & Research reported $56 billion[2] in losses due to identity theft-related cybercrimes. For individuals, the effects of cybercrime can be severe, leading to significant financial loss, as well as damage to trust and reputation.

1. How aligning security and the business creates cyber resilience, State of Cybersecurity Resilience 2021. On site: https://www.accenture.com/content/dam/accenture/final/a-com-migration/pdf/pdf-165/accenture-state-of-cybersecurity-2021.pdf
2. Report: The 2021 Identity Fraud Study, BY ALEX ROLFE, April 2021, on site: https://www.paymentscardsandmobile.com/report-the-2021-identity-fraud-study/

01

Chapter One

Concept of Cyber Forgery and Fraud and Its Types

- **First:** Concept of Cyber Fraud
- **Second:** Reasons for Falling Victim to Cyber Fraud
- **Third:** Types and Forms of Cyber Fraud

First: Concept of Cyber Fraud

Cyber fraud is one of the most prevalent cybercrimes, significantly facilitated by the increase in internet users and the expansion of digital applications, such as electronic payment methods, social media and others. Phishing and fraud crimes targeting individuals have increased alongside the growing number of internet users and its integration into all aspects of economic, commercial, political, and social life. Consequently, work, shopping and entertainment can now be easily and quickly conducted online via a smartphone connected to the internet.

Cyber fraud is one of the simplest cybercrimes to commit, since it does not require specialised skills or software, or expertise in hacking. It often occurs through social media accounts via impersonation and chatroom scams. Cyber fraud refers to deception or tricks carried out over the internet, commonly taking place in chatrooms, emails, forums, or websites, targeting users to steal funds, personal information, and other data. Usually, online fraud attacks are driven by motives such as espionage, impersonation, or acquiring account information of users in senior positions or in connection with key individuals (i.e., for personal reasons). Additionally, attacks can involve stealing funds from bank accounts and electronic payment cards[1].

Facts and Information

Your digital footprint comprises various online activities, including shopping and site registrations.

[1] Internet Fraud, Australian Federal Police (AFP). on site: https://police.act.gov.au/sites/default/files/PDF/bizsafe-internet-fraud-factsheet.pdf

The hacking process (online fraud) usually occurs when individuals visit websites, chat rooms (messengers), online stores, blogs, or mobile applications. During this stage, the victim is caught in a digital trap, enabling the attacker to continue with their illegal activities by compromising personal data and customer accounts.

Definition of Cyber Fraud

Cyber fraud is the deliberate manipulation of valuable information and data stored in a computer system, or the unauthorised input of accurate information and data, manipulation of commands and instructions through programming or other means. This manipulation causes the computer to perform actions based on these commands, data, or instructions to obtain illegal profits and inflict harm on others. The criminal activity can be managed remotely, away from the crime scene, or even outside the country, such as in cases of fraud involving the promotion of inappropriate content or electronic scams[1].

Online fraud is linked to several related concepts, such as informational fraud, which refers to deception or manipulation within information processing systems to unlawfully acquire services, money or specific assets. Another related concept is "electronic financial fraud or scam" which involves the fraudulent seizure of another person's money through deceptive means, resulting in the theft of funds through computer systems.

In such cases, the perpetrator, known as the "cyber attackers," employs advanced techniques to manipulate banking data, financial entitlements, and company budgets to swiftly transfer money to their own account. This type of cyberattack can have a negative impact on the national economy, potentially leading to the bankruptcy of banks and businesses.

[1] Younis Al-Basha, Fayza. Organized Crime in Light of International Agreements and National Laws, Dar Al-Nahda Al-Arabiya for Printing, Publishing, and Distribution, 2001, p. 21.

Second: Reasons for Falling Victim to Cyber Fraud

There are various reasons for falling victim to online fraud, often stemming from improper social media and internet usage, and a lack of adherence to safe online practices or understanding of cybersecurity and digital safety concepts.

Facts and Information

You can protect your digital footprint by reviewing privacy settings and avoiding insecure sites.

The following highlights the main factors and causes leading internet users to fall victim to online fraud:

- ✓ Lack of awareness about the importance of safe internet practices.
- ✓ Impulsive decision-making while browsing websites or opening emails. Users may hastily click on links, a strategy frequently used by online fraudsters to catch victims off guard and prevent them from verifying the legitimacy of a message.
- ✓ Visiting unsafe websites where users encounter fake notifications or messages claiming they have won money or smart devices. These prompts often encourage users to provide personal information to claim a prize, leading to fraud once their details are submitted.

- Sharing personal information on social media platforms, which provides fraudsters with valuable data that can be used to deceive and exploit users.
- Interacting with fraudulent online stores seeking to deceive users and steal money from their payment cards.
- The rise of cryptocurrency exchange platforms, such as Bitcoin. While many platforms are legitimate, some are fraudulent, initially offering small returns to build trust, only to later steal funds from users.
- Fraudsters impersonating public figures or officials to attract and deceive internet users.
- Exploiting human compassion: Some fraudsters pretend to represent organisations or individuals seeking donations for urgent humanitarian cases, aiming to defraud users. Therefore, donations should only be made to recognised organisations with official websites and receipts.

Did you know?

Public networks are not secure and may expose you to hacking.

Third: Types and Forms of Cyber Fraud

Types of Cyber fraud are not fixed or permanent, as fraudsters frequently evolve their methods. However, most scams occur using certain primary tools and techniques **The following outlines the most notable tools and types.**

Email:

Emails may contain links to enticing competitions or prizes, such as smartphones or the opportunity to spend a holiday in a foreign country. Once the link is clicked, the email owner may be asked to enter personal or financial information, such as their credit card number, national ID number, passport number, or other important personal details. A small money transfer may also be requested to claim the prize. This exposes personal information to risk and increases the chances of funds being stolen from private accounts.

One of the most deceptive and manipulative Cyber fraud tactics involves sending a fraudulent email that appears to come from a trusted friend or legitimate organisation. It is a phishing attempt to steal personal and sensitive information. The email may claim that your PayPal account is breached and urges you to change your password. The message appears to be from the legitimate site, which increases the chances that the user will follow through and reset their password. This allows the fraudster to gain access to your account and steal your funds[1].

[1] What is email fraud? Cloudflare. On site: https://www.cloudflare.com/learning/email-security/what-is-email-fraud/

Smartphone:

Installing unsafe applications or clicking on unknown links (from unknown or suspicious sources) can expose personal data, such as photos and files, and lead to the theft of sensitive information, like passwords and bank card details. This can make individuals vulnerable to cybercriminals, who may exploit their personal information for illegal activities. Additionally, Cyber fraud can occur when a criminal impersonates an online friend using the same name and profile picture to request favours, such as transferring money to a phone number or utilising personal data[1].

Facts and Information

Verifying unknown links before clicking on them reduces the possibility of falling victim to fraud.

[1] Mobile phone fraud, Action Fraud – National Fraud & Cyber Crime Reporting Centre. On site: https://www.actionfraud.police.uk/a-z-of-fraud/mobile-phone-fraud

Computer:

Computers in large and small companies and organisations often contain highly valuable information, making them targets for hackers and fraudsters who use malware and malicious links to disrupt operations. Then, the attackers contact the owners of these companies or organisations, demanding payment in exchange for restoring access to their accounts and retrieving the stored information[1].

E-Commerce:

With the growth of e-commerce, a new form of online fraud has emerged, targeting victims who shop on commercial websites. A user may visit a fake site intending to purchase goods, only to find themselves victims to Cyber fraud[2] and paying for items they never receive. Additionally, some fraudulent websites may redirect users to unknown electronic payment platforms with the intent of stealing their banking information.

[1] Computer and Internet Fraud, Impact Law. On site: https://www.impactlaw.com/criminal-law/white-collar/computer-internet-fraud/

[2] Varga, Gergo. 7 Types of Ecommerce Fraud & How to Detect Them, SEON. On site: https://seon.io/resources/ecommerce-fraud-detection-and-prevention/

Exploiting Disasters:

During crises such as natural disasters or health emergencies, like the “COVID-19 pandemic” occurred a few years ago, cybercriminals organise fake campaigns calling for donations to help victims. This leads to the victims providing their banking account information, falling under the category of online fraud.

Facts and Information

Creating unique and strong passwords for each account prevents hackers from accessing your other accounts if one password is leaked.

02

Chapter Two

How Cyber Fraud is Executed

- **First:** Vulnerabilities Resulting in Cyber Fraud
- **Second:** Personal Data Security and Cyber Fraud
- **Third:** Digital Footprint and Cyber Fraud

First: Vulnerabilities Resulting in Cyber Fraud

Digital vulnerabilities are among the factors contributing to the risk of becoming a victim of cyber fraud. A digital vulnerability is a term referring to weak spots in computer operating systems. These weak areas can be exploited to penetrate the operating system, allowing attackers to alter it, either to destroy it or to spy on private information belonging to the computer's owner, also known as the victim's device.[1] Security vulnerabilities also appear in all software, not only in operating systems, due to coding errors during development by programmers. These vulnerabilities pose a security risk due to their frequent undetected nature, necessitating a new release to address the flaw. These undiscovered vulnerabilities, known as **Zero-day vulnerabilities**, are often used by hackers in cybercrimes. A Zero-day vulnerability is a defect in software that can be exploited by unauthorised intruders but remains undetected by developers, who either fail develop a patch to fix it or neglect it, leading to significant cybersecurity breaches.[2]

[1] What is bug? Neterich. On site: https://netenrich.com/glossary/bug

[2] What is a Zero-day Attack? - Definition and Explanation, Kaspersky. On site: https://www.kaspersky.com/resource-center/definitions/zero-day-exploit

Examples of Zero-Day Attacks

Here is an example of security vulnerability attacks that illustrate the potential risks they pose to organisations and individuals.

Sony

In 2014, a Zero-day attack targeted Sony Pictures, resulting in the destruction of Sony's internal network and the leak of sensitive company data on file-sharing sites. This included personal information about Sony employees and their families, internal communications, CEO salaries and unreleased Sony films. The attackers used a distinct type of malware to wipe multiple systems on Sony's network.[1]

Wanna Cry Attack

This attack affected over 200,000 devices worldwide in a single day in May 2017. The ransomware spread through computers running Microsoft Windows, taking control of users' files and demanding Bitcoin ransom for their return. The vulnerability stemmed from users' failure to update their outdated systems. The attackers exploited a known vulnerability in Microsoft Windows with a technique known as "Eternal Blue."

[1] VB2018 paper: Since the hacking of Sony Pictures, Minseok (Jacky) Cha, AhnLab, South Korea. On site: https://www.virusbulletin.com/virusbulletin/2018/11/vb2018-paper-hacking-sony-pictures/

Two months before the attack, Microsoft released a security update to protect users' systems. However, many failed to regularly update their systems, making them prime targets. The attackers initially demanded a ransom of $300 in Bitcoin, later raising it to $600 per individual to restore users' files[1].

Did you know?

Sharing photos and personal information online increases the risk of being tracked and having your data exploited in unsafe ways.

✓ Untargeted Zero-day Attacks

A notable type relevant to individuals is untargeted Zero-day attacks. These attacks are usually launched against many home users (ordinary individuals) using vulnerable systems, such as operating systems or browsers. The attacker's goal is often to compromise these systems for later use in creating extensive bot networks for larger cybercrimes. [2]

1. What was the WannaCry ransomware attack? cloudflare. On site: https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/
2. Zero Day Exploit: All You Need to Know, phoenixnap, 2023. On site: https://phoenixnap.com/blog/zero-day-exploit#:~:text=A%20zero%2Dday%20exploit%20is,vendor%20learns%20about%20the%20vulnerability.

Second: Personal Data Security and Cyber Fraud

Information security refers to a set of security measures and tools designed to broadly protect sensitive information from misuse, unauthorised access, disruption, or destruction. Information security encompasses physical and environmental security, access control and online security.[1]

Meanwhile, data theft is the act of stealing digital information stored on computers or phones to obtain confidential information or breach privacy. The stolen data can include bank account information, online passwords, passport numbers, medical records, online subscriptions, etc. Once an unauthorised person gains access to personal information, they can delete, alter, or prevent access to it without the owner's permission.[2]

Data theft often occurs due to individuals' desire to sell the information or use it for identity theft. If data criminals can steal sufficient information, they can use it to access secure accounts, issue credit cards in the victim's name, or misuse the victim's identity in other ways for their benefit. In the digital world, the term "theft" does not literally mean taking information away from the victim. Instead, it refers to simply copying the information for the attacker's use. This type of cybercrime is known as a "data breach" or "data leak.

[1] What is Information Security?", Microsoft. Available at: https://www.microsoft.com/ar/security/business/security-101/what-is-information-security-infosec

[2] What is Data Theft and How to Prevent It?", Kaspersky. Available at: https://me.kaspersky.com/resource-center/threats/data-theft

Facts and Information

Adjusting privacy settings on social media sites reduces the sharing of your information with unknown parties.

The most common form of this type of crime is phishing, which occurs when a fraudster poses as a trusted entity to deceive the victim into opening an email, text, or instant message containing malware. Individuals who fall victim to phishing attacks are vulnerable to identity theft.

Individuals can also expose themselves to online fraud by downloading programmes or files from compromised websites infected with viruses, such as mobile viruses or malware. This provides criminals unauthorised access to their devices, allowing them to steal data.

Third: Digital Footprint and Cyber Fraud

The term “digital footprint” or “digital shadow” refers to the data trail created through online activity, whether deliberately or inadvertently. This footprint encompasses various forms of data, including the websites you visit, the emails you send or receive, and the details you provide when registering, shopping or interacting online.[1]

A digital footprint also encompasses other activities, such as posting on social media, subscribing to newsletters, leaving online reviews or shopping online. Additionally, websites record user activity through cookies, installed on devices to track online behaviour. Many applications similarly collect user data, sometimes without full user awareness, making this information part of their digital footprint.

Once access to your data is granted to a third party, it can be utilised in multiple ways, such as selling it to marketing firms or sharing it with other entities. In certain cases, this data may be used to deliver personalised advertisements or to gather additional information about you. More concerningly, such information might lead to security breaches or identity theft, placing your privacy and personal security at significant risk.

[1] What is a digital footprint? And how to protect it from hackers, Kaspersky. On site: https://www.kaspersky.com/resource-center/definitions/what-is-a-digital-footprint

Examples of Digital Footprints

Users may leave digital footprints through various online activities. Below are some examples of these activities:

- ✓ Online shopping.
- ✓ Purchasing from e-commerce websites.
- ✓ Registering to create an account on a specific website.
- ✓ Downloading and using shopping applications.
- ✓ Subscribing to brand newsletters.
- ✓ Online banking services.
- ✓ Using mobile banking applications.
- ✓ Subscribing to publications and blogs.
- ✓ Opening a credit card account.
- ✓ Using social media on your personal devices.
- ✓ Logging into other websites using social media credentials.
- ✓ Communicating with friends and contacts online.
- ✓ Sharing information, data and images with acquaintances.
- ✓ Subscribing to an online news source.
- ✓ Reposting information you read.
- ✓ Using fitness tracking devices.

Digital Footprint Protection

Here are some tips for protecting personal data and managing personal online reputation.

✓ Checking Digital Footprints via Search Engines

This involves users deliberately sharing information about themselves, such as posting or sharing on social platforms Individuals can review publicly accessible information by searching their name in search engines. If any results portray them negatively, they may contact the website administrator to request removal. Setting up Google Alerts is an effective way to monitor one's name.(1)

✓ Reducing Sources of Information

Websites often contain more information than individuals might want displayed. These sites may include personal information like phone numbers, addresses and ages. Therefore, individuals should regularly remove personal information from such sites.

✓ Limiting Shared Data

Each time we provide personal information to an organisation, we create a digital footprint and increase the risk of data misuse or breach, potentially exposing our data to unauthorised parties. Therefore, it is prudent to consider carefully before sharing any information online.

1. How to protect your digital footprint, state farm, 2023. On site: https://www.statefarm.com/simple-insights/family/how-to-reduce-and-protect-your-digital-footprint

Reviewing Privacy Settings

Social media privacy settings allow users to control who sees their posts. It's advisable to review these settings and ensure they are configured according to one's preferences. For example, **Facebook** allows users to limit posts to friends or create customised lists for specific audiences.

Carefully Sharing Information on Social Media

Social media facilitates connection; however, it enables oversharing of personal information. It's crucial to think carefully before disclosing location or other personal details like phone numbers or email addresses.

Avoiding Unsecure Websites

Each time we access the internet, we should ensure we engage with a secure website. URLs beginning with https:// (as opposed to http://) signify security, with the "s" indicating "secure." A lock icon to the left of the address bar also denotes a secure site.

Facts and Information

Deleting old, unused accounts reduces the risk of personal data exploitation.

✓ Be Cautious with Public Wi-Fi

Public Wi-Fi networks are inherently less secure than private ones, as we cannot be sure who set them up or who else may be monitoring them. Personal information should be avoided when using public Wi-Fi.

✓ Deleting Old Accounts

A key approach to reducing our digital footprint is to delete outdated accounts, such as inactive social media profiles or newsletter subscriptions we no longer engage with.

✓ Creating Strong Passwords and Using a Password Manager

A strong password should be at least 12 characters long, ideally more, and contain a mix of uppercase and lowercase letters, symbols and numbers. The more complex and challenging a password is, the harder it is to crack. Password managers assist in generating, storing and managing all passwords within one secure online account.

✓ Avoid Logging in with Facebook

Logging into websites and applications using **Facebook** credentials is convenient. However, it grants these third parties' access to view and retain personal data, potentially putting personal information at risk.

✓ Regularly Updating Software

Outdated software may contain a wealth of digital footprints. Without the latest updates, cybercriminals may exploit these vulnerabilities to access a victim's data and devices. Frequent software updates help secure systems, as older versions may be more susceptible to hacker attacks.

✓ Setting a Password for Mobile Devices

Ensure a passcode is set for mobile devices to prevent unauthorised access in case of loss. Additionally, when installing an app, carefully read the user agreement, as many apps disclose the types of data they collect and how it might be used. Such apps may store personal data like email, location and online activities.

✓ Immediate Action After a Data Breach

If personal data is suspected to be compromised, immediate action is necessary, especially in cases of financial loss. The first step is to change any potentially exposed passwords. If the same password is used across accounts, it should be updated as well.[1]

[1] How to Map, Monitor and Manage Your Digital Footprint, Bitdefender. On site: https://www.bitdefender.com/en-us/cyberpedia/how-to-protect-your-digital-footprint

Using a VPN

A Virtual Private Network (VPN) helps protect digital footprints by masking one's IP address, rendering online actions practically untraceable. This protects online privacy and prevents websites from tracking internet browsing history through cookies.

03

Chapter Three

How to Avoid Cyber Fraud

First: Cyber Fraud Prevention Guidelines

Fraudsters continuously develop new methods to implement cybercrimes, but some simple steps can enhance information security. The key steps include:

- ✓ **Downloading Apps from Trusted Stores**

  All apps should be downloaded from reputable stores, as downloading from unknown sources could lead to data and privacy theft.

- ✓ **Updating Phone Applications**

  Installing the latest updates for the phone's operating system is essential, as these updates often include files that strengthen protection against various forms of hacking.

- ✓ **Avoiding Suspicious Links**

  Even if the links are sent by friends, clicking on them could expose your device to hacking or the installation of malware without your knowledge. Additionally, avoid opening emails from unknown senders.

Being Cautious with Third-Party Transactions

Caution should be taken when requesting to receive any financial transfers and subsequently forwarding them to a third party, as this could be part of a fraud or money laundering scheme.

Using Antivirus Software

It is crucial to install reputable antivirus software on smartphones and computers to enhance device security.

Using Complex Passwords

Passwords should include letters, symbols and numbers and be changed immediately if there is any suspicion of compromise.

Did you know?

Using complex and unique passwords can greatly reduce the risk of your personal accounts being hacked.

Avoid Shopping on Unknown Sites

Only make online purchases from reputable and well-known websites. If there are doubts about the credibility of a site, further research is necessary to verify its legitimacy.

Second: Data Protection from Cyber Fraud

Protecting personal and financial data from fraud is achievable through several measures, including:

- ✓ Be alert to potential fraud when dealing with unsolicited communications from individuals or entities, whether through phone, mail, email, or social media platforms, as they may be fraudulent attempts.
- ✓ If you've met someone online, take the time to verify their identity by searching for their pictures on **Google** Images or looking up other individuals who may have had interactions with them.
- ✓ Avoid opening suspicious texts, pop-up windows, or emails. Always verify the identity of the sender through an independent source, such as conducting an online search.
- ✓ Keep your personal details secure by locking your mailbox and storing passwords and PINs in a safe place. Be cautious of the personal information you share on social media platforms.
- ✓ Regularly update your phone and computer systems and maintain data backups.
- ✓ Set a password for your Wi-Fi network and avoid using public computers or Wi-Fi hotspots.
- ✓ Regularly review privacy and security arrangements on social media platforms.

- ✓ Be cautious with any requests involving your details or money.
- ✓ Be cautious of unusually attractive online offers when shopping online.
- ✓ When reviewing a new profile, be attentive to anything unusual in the other person’s information, such as their **image, location, interests, or language skills.** Fraudsters often use fake images they find online, so perform an image search to confirm that the person is indeed who they claim to be. You can search for pictures on **Google** Images.
- ✓ If there is suspicion of a compromised computer or phone, conduct a thorough system scan with trusted antivirus software and change passwords. This should also be done for online accounts, whether on social media, shopping sites or others; password should be changed immediately.
- ✓ Bookmarking important sites by adding the frequently visited sites in your bookmarks and access them only from there to eliminate the risk of accidentally opening fake pages.
- ✓ Several warning signs can help identify counterfeit documents, such as “bank account details” or “flight bookings,” which may serve as traps set by cybercriminals disguised as fraudulent gifts to extract personal information. These signs include generic greetings instead of personalised ones, the use of non-existent organisation names, poor formatting, weak grammar and spelling, and excessive formality.

- ✓ Remember that legitimate error messages from companies like **Microsoft** or other major tech companies never include phone numbers to call.
- ✓ Microsoft or other reputable tech companies will never contact you to inform you of issues with your device. Unless you contact them first, technical support agents will not require your social security number or any other unrelated personal information. If you receive an unsolicited call offering technical support, end the call immediately.
- ✓ If your screen suddenly fills with alarming pop-up windows, close your browser immediately **(try pressing ALT+F4 if you cannot do so with your mouse)**. If you are unable to close the browser, try restarting your computer.[1]

Did you know?

Avoiding logging in with Facebook data protects your digital footprint from unnecessary exposure.

[1] Protect yourself from online scams and attacks, Microsoft, on site: https://support.microsoft.com/en-gb/office/protect-yourself-from-online-scams-and-attacks-0109ae3f-fe61-4262-8dce-2ee3cd43bac7

Exercises

Exercises in this part are based on the presented material.

An answer key is provided at the end of the booklet.

Exercise 1

Choose the Correct Answer

1. Which of the following is an example of an active digital?

1 Social media posts.

2 Location tracking applications.

3 Websites installing cookies without user notification.

2. Reasons for internet fraud include

1 Misuse of online platforms.

2 Proliferation of fake online stores.

3 Exploiting sympathetic feelings.

4 All the above.

3. The term “theft” in the internet realm refers to ....

1 Data breach.

2 Data leakage.

3 All the above.

4. To track someone’s online activities, you can use ....

1 Facial recognition.

2 Handprint.

3 Digital footprint.

Exercise 2

Provide the Correct Term or Phrase for the Following Descriptions

1. An attack we experience that disrupts our online accounts, requiring a ransom for access restoration.

2. Emails or messages promising fake monetary rewards or gifts intended to deceive and steal our data.

3. Vulnerabilities that lead to the compromise of our devices, whether computers or phones, and expose us to risk.

4. Tools that safeguard sensitive information from unauthorised access, disruption, or damage.

5. A unique type of theft targeting our personal online data, punishable by law.

6 Digital traces on the internet are exploited by attackers to leverage the sensitive information and data they contain, deceiving us and others.

7 Composed of 12 characters, symbols, and numbers, designed to protect us online.

Exercise 3

Complete the Sentences with the Correct Answer

1 ....digital footprint refers to users sharing information about themselves intentionally.

2 .... digital footprint refers to data collection about users without their awareness.

3 Cybercriminals can exploit .... for impersonation purposes.

4 One of the ways users add to their digital footprint is by downloading ....

5 Limiting .... is a way to protect your digital footprint.

6 Checking privacy settings is a method to safeguard ....

7 One safety guideline for avoiding online fraud is to avoid clicking on ....

8 It is preferable to use passwords consisting of .... to protect against online fraud.

9 In case of online fraud, you should report to ....

10 If your screen suddenly fills with alarming pop-up windows, you should ....

Answer Key

Question

Exercise 1: Choose The Correct Answer

Answer

1 Social media posts

2 All the above

3 All the above

4 Digital footprint

Question

Exercise 2: Provide The Correct Term Or Phrase For the Following Descriptions

Answer

1 Ransomware

2 Cyber fraud

3 Security gaps

4 Information security

5 Data breach

6 Digital footprint

7 Password

Question

Exercise 3: Complete The Sentences With The Correct Answer

Answer

1 Active Digital footprint refers to users sharing information about themselves intentionally.

2 Passive Digital footprint refers to data collection about users without their awareness.

3 Cybercriminals can exploit digital footprint for impersonation purposes.

4 One of the ways users add to their digital footprint is by downloading applications.

5 Limiting data shared is a way to protect your digital footprint.

6 Checking privacy settings is a method to safeguard digital footprint.

7 One safety guideline for avoiding online fraud is to avoid clicking on unknown source.

8 It is preferable to use passwords consisting of letters, symbols, numbers to protect against online fraud.

9 In case of online fraud, you should report to trusted individuals, such as parents.

10 If your screen suddenly fills with alarming pop-up windows, you should close it immediately.

References

1. Younes Al-Basha, Fayza. Organized Crime in Light of International Agreements and National Laws, Dar Al-Nahda Al-Arabiya for Printing, Publishing, and Distribution, 2001, p. 21.
2. “What is Information Security?”, Microsoft. Available at: https://www.microsoft.com/ar/security/business/security-101/what-is-information-security-infosec
3. “What is Data Theft and How to Prevent It?”, Kaspersky. Available at: https://me.kaspersky.com/resource-center/threats/data-theft
4. How aligning security and the business creates cyber resilience, State of Cybersecurity Resilience 2021. On site: https://www.accenture.com/content/dam/accenture/final/a-com-migration/pdf/pdf-165/accenture-state-of-cybersecurity-2021.pdf
5. Report: The 2021 Identity Fraud Study, BY ALEX ROLFE, April 2021, on site: https://www.paymentscardsandmobile.com/report-the-2021-identity-fraud-study/
6. Internet Fraud, Australian Federal Police (AFP). on site: https://police.act.gov.au/sites/default/files/PDF/bizsafe-internet-fraud-factsheet.pdf
7. What is email fraud? Cloudflare. On site: https://www.cloudflare.com/learning/email-security/what-is-email-fraud/
8. Mobile phone fraud, Action Fraud – National Fraud&Cyber Crime Reporting Centre. On site: https://www.actionfraud.police.uk/a-z-of-fraud/mobile-phone-fraud

9. Computer and Internet Fraud, Impact Law. On site: https://www.impactlaw.com/criminal-law/white-collar/computer-internet-fraud/

10. Varga, Gergo. 7 Types of Ecommerce Fraud & How to Detect Them, SEON. On site: https://seon.io/resources/ecommerce-fraud-detection-and-prevention/

11. What is bug? Neterich. On site: https://netenrich.com/glossary/bug

12. What is a Zero-day Attack? - Definition and Explanation, Kaspersky. On site: https://www.kaspersky.com/resource-center/definitions/zero-day-exploit

13. VB2018 paper: Since the hacking of Sony Pictures, Minseok (Jacky) Cha, AhnLab, South Korea. On site: https://www.virusbulletin.com/virusbulletin/2018/11/vb2018-paper-hacking-sony-pictures/

14. What was the WannaCry ransomware attack? cloudflare. On site: https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/

15. Zero Day Exploit: All You Need to Know, phoenixnap, 2023. On site: https://phoenixnap.com/blog/zero-day-exploit#:~:text=A%20zero%2Dday%20exploit%20is,vendor%20learns%20about%20the%20vulnerability.

16. What is a digital footprint? And how to protect it from hackers, Kaspersky. On site: https://www.kaspersky.com/resource-center/definitions/what-is-a-digital-footprint

17. How to protect your digital footprint, state farm, 2023. On site: https://www.statefarm.com/simple-insights/family/how-to-reduce-and-protect-your-digital-footprint

18. How to Map, Monitor and Manage Your Digital Footprint, Bitdefender. On site: https://www.bitdefender.com/en-us/cyberpedia/how-to-protect-your-digital-footprint

19. Protect yourself from online scams and attacks, Microsoft, on site: https://support.microsoft.com/en-gb/office/protect-yourself-from-online-scams-and-attacks-0109ae3f-fe61-4262-8dce-2ee3cd43bac7

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative