Forgery and online fraud

Trainer’s booklet

Middle School

CyberEco

معًا لدعم السلامة الرقمية
Together to support digital safety

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

Forgery and online fraud

Middle School

Training kit

Trainer's booklet

Intellectual Property rights

December, 2023
Doha, Qatar

This content is produced by the team of
National Cybersecurity Excellence Management, National Cyber Security Agency.

For inquiries about the initiative or program, you can contact us through the following websites or phone numbers:

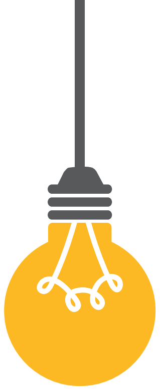
الوكالة الوطنية للامن السيبراني
National Cyber Security Agency

🌐 https://www.ncsa.gov.qa/
✉ cyberexcellence@ncsa.gov.qa
📱 00974 404 663 78
📱 00974 404 663 62

General content of the Kit

First: General Introduction to the training kit

Second: Scientific content



First: General Introduction to the Training Kit

Below is an explanation of some details relevant to the objectives of the training kit, along with general guidelines for the trainer on how to handle this kit, while providing him with the scientific content that will be relied upon during the training.

General idea

The concept of this training kit is to equip the trainer with tools and training resources, making it easier for him to deliver information to the trainees. In general, each training material consists of two parts: One part for the trainee and another for the trainer. The training kit serves as a general guide and support for the trainer, and its scientific content is the same as that of the trainee, but here the training content is presented differently. Additionally, the kit equips the trainer with training tools and methods that support him in the training process.

Objectives of the Training Kit

- Providing the trainer with training tools that help him deliver the training content to the students.
- To present information and training content in an easy and simple manner.
- To offer training content on forgery and online fraud along with multiple training tools and methods.

Contents of the Training Kit

The training kit includes several training tools, as detailed below:

1. **Presentation files.**
2. **Training games,** such as shape coloring, drawings and crossword puzzles, which the trainer presents to the students to ensure their interaction with the training content.
3. **Educational videos.**
4. **Competitions,** Contests in the form of inferential questions presented by the trainer to encourage interaction between the students.
5. **Training cards,** comprising general information accompanied by illustrative images, presented by the teacher to the students. Currently, the content of the training cards is being prepared, and will later be designed in the form of cards.
6. **Sketches,** including information about the main topics in the training content.

Content of the Training Kit

WorkShop Timetable

Content	Content
General introduction	5 minutes
The theoretical aspect	25 minutes
Educational Videos	25 minutes
Short break	20 minutes
Training games	25 minutes
Dialogue and discussion with students	15 minutes
Graduation project	5 minutes
Total training time	2 hours

Trainer's Guidance Manual

The following is an explanation of some general guidelines for the trainer, revolving around how to use this training kit:

1. The scientific content of the kit may exceed the children's ability to comprehend, especially in terms of general concepts. Therefore, the trainer must simplify these concepts and present them in a way that is understandable to middle school students.
2. The trainer presents slides for each point discussed. For example, when talking about the concept of forgery and online fraud, the first slide is displayed: what is forgery and online fraud?
3. After explaining the scientific material, a simple test is given to them, such as "Mark (✓) or (✗) for each sentence.
4. During the explanation of the first chapter, specially designed images for the "Did you know that..?" section are distributed.
5. The trainer presents sketches to the students while they solve the exercises.
6. At the end of the training, the mentioned competition questions are presented.
7. During the presentation of the scientific material for each chapter, a portion of the allocated time is used to present several links related to the content of the chapter.
8. The trainer presents the videos - mentioned in a separate file- to the students at the end of each chapter or at a time they deem appropriate.
9. Examples of incidents related to forgery and online fraud, are mentioned during the presentation of the scientific material.
10. It is encouraged to open a discussion with the students to hear their opinions.
11. Regarding exercises directed towards students; a file with exercises will be attached at the end of this kit. These exercises are divided into two parts: a part to be given to students during training, which are classroom exercises, and the other part assigned for students to answer at home, which are non-classroom exercises. This division will be explained at the end of this kit.

Graduation Project

The graduation project is a task carried out by the student, aimed at achieving several goals, Here is an explanation of the most important ones:

- Ensure that the student has absorbed the information and ideas presented and is capable of applying them in their daily life.
- Consolidate the information and ideas that were presented to the student.
- The project serves as a link between theoretical information and practical real-world application.

Regarding the mechanism for assigning students to the project, and how to implement it, the following guidance can be provided:

- The graduation project can be individual or group-based, In case of a group project; the number of students participating in one project should not exceed three students.
- The students choose the project topic, and the trainer can provide some assistance or ideas in this field.
- The topic of the graduation project must be consistent with the training content that was presented to the students.
- The graduation project can be within one of the following scenarios, which are non-binding concepts. The trainer can choose other concepts that he find suitable. Here are some suggestions:
  - Writing a short story about a student who has experienced attempted online fraud and the student will write about how he dealt with it.
  - The student takes on the role of the trainer and writes general guidelines for his colleagues or parents, explaining the procedures required to prevent the risks of forgery and online fraud.

Second: scientific content

Introduction

In the current digital explosion in our world, we are all exposed to various newly-coined terms associated with the realm of crime. This includes cybercrimes targeting computers and networks, seeking to exploit them for criminal activities to make money or cause harm to their owners for personal reasons. Most cybercrimes are committed by hackers or cybercriminals.

There are many types and forms of cybercrime, , such as fraud through email and the internet, identity theft, where personal information is stolen and misused, Financial data theft, or credit card data, and electronic extortion, where certain individuals are are threatened in exchange for money, and this type of crime is also called ransomware attacks. In addition to crimes of copyright infringement, the sale of illegal goods via the internet.

According to Accenture's Cyber Threat Report for 2021, digital attacks increased by 31% between 2020 and 2022, and the number of attacks per company increased from 206 to 270 annually. These attacks also affect individuals as well, as many companies retain critical data and personal information belonging to their clients. A single attack, whether it is data breach, malware, ransomware, or a denial-of-service attack, can cost companies, on average, around $200,000 regardless of their size [1].

In 2021, Javelin Strategy & Research published a study on identity fraud revealing that the losses from this type of cybercrime reached $56 billion[2]; as for individuals, the impact of cybercrime cybercrime can be deep, causing primarily financial damage and also leading to loss of trust and damage to reputation.

1. How aligning security and the business creates cyber resilience, State of Cybersecurity Resilience 2021. On site: https://cutt.us/ZMXpW
2. Report: The 2021 Identity Fraud Study, BY ALEX ROLFE, April 2021, on site: https://cutt.us/fVN5g

Chapter One

The Concept of Forgery and Online Fraud and Its Types

- First: The concept of online fraud
- Second: Reasons for falling victim to online fraud
- Third: Types and forms of online fraud

01

First: The concept of online fraud

Online fraud is one of the most widespread forms of cybercrime. Its prevalence has increased in recent years due to the growing number of internet users and various applications, such as electronic payment methods, and the widespread use of social media and others.This surge in online fraud and phishing attacks aligns with the rise in internet users' involvement in all aspects of economic, commercial, political, and social life. Work, shopping, and entertainment have become easily and rapidly accessible through the internet using a smartphone.

Online fraud is one of the easiest cybercrimes to commit because it does not require experts, specialized programs or hackers, but this crime is achievable through social media accounts via identity theft and fraudulent activities in chat rooms. online fraud is considered a form of deception and trickery that are carried out on the internet, and these crimes often occur in chat rooms, via e-mail, on forums or websites (web).

The goal of these crimes is to defraud customers and users by stealing money, important personal information and other data; Fraudulent activities are usually aimed at espionage, identity theft or obtaining user account information in important positions or related to important people (i.e. for personal reasons), and may be for stealing funds from bank accounts and electronic payment cards [1].

The breach (online fraud) usually takes place when individuals visit websites, chat rooms (Messenger), online stores, blogs or smart applications, and at this stage the victims are lured into an online trap, allowing criminals to execute their illegitimate plan by attacking people's data and customer accounts.

1. Internet Fraud, Australian Federal Police (AFP). on site: https://cutt.us/leAYp

Definition of online fraud crime

Online fraud crime is defined as the intentional manipulation of information and data that represent tangible value stored within the computer system, or the unauthorized input of accurate information and data, manipulation of commands and instructions through programming process or any other means, which would influence the computer to perform operations based on these instructions, data, or commands in order to obtain illegal profit and causing harm to others. The management of these criminal activities can occur remotely, away from the actual crime scene, or outside the boundaries of the state, such as in cases of fraudulent activities related to the promotion of inappropriate materials and online fraud [1].

Online fraud is associated with various other concepts, such as the concept of information fraud, which means: Deception or fraudulent manipulation of information processing systems, with the intention of wrongfully gaining access to services, money, or specific assets.; as well as the concept of "Scam or online financial fraud", which means: Seizing others' money through deceitful means, often involving the use of computers.

In these cases, the perpetrators, known as "cyber attackers," utilize advanced techniques to manipulate financial data, financial entitlements, and corporate budgets to transfer money swiftly into their personal accounts. This type of cyberattacks adversely affects the national economy as it can lead to bankruptcies of banks and companies.

[1] Younes El-Basha, Fayza. Organized Crime in the Context of International Agreements and National Laws, Dar Al-Nahda Al-Arabiyya for Publishing, Printing, and Distribution, 2001, p. 21.

Second: Reasons for falling victim to online fraud

There are multiple reasons leading to online fraud crimes, often due to the misuse of social media and the internet, not following safe internet usage practices, and lack of full awareness of cybersecurity and digital safety concepts.

Here is an explanation of the main factors and reasons that lead internet users to fall victim to online fraud:

- Lack of awareness of the importance of safe internet usage practices.
- Rushing to make a decision when browsing websites, or opening emails; users might impulsively interact with any link presented to them, a technique used by online scammers to prevent the targets from thinking or verifying the authenticity of the received message.
- Accessing unsafe websites, where users receive fake notices or messages, often indicating that the user has won money or electronic devices, then asking for personal data; providing personal data in this scenario would make the user a victim of fraud.
- Sharing personal information on social media and online platforms, which can be exploited by fraudsters to deceive and defraud users based on their digital footprint.
- Dealing with fake online stores that seek to deceive users and steal money from their electronic payment cards.
- The spread of digital currency exchange platforms, such as Bitcoin and others, some platforms are fake and deceive users, occasionally offering them money to gain their trust, then later deceiving and stealing their money.
- Impersonation of official or public figures, which sometimes attracts internet users, and later leads to their deception.
- Exploiting human sympathy, some fraudsters may impersonate organizations or individuals collecting donations for urgent humanitarian cases, some of which are fraudulent, so any donations or assistance should only be provided to well-known organizations with official websites and based on certified receipts.

Third: Types and Forms of Online Fraud

There are no fixed or permanent types of online fraud, Scammers often seek to develop their methods, but in general they occur through major tools and means.

Here is an explanation of the most important tools and types:

E-mail address

E-mail may receive messages containing links to contests or attractive financial and in-kind prizes such as: smartphones or a chance to spend holidays in a foreign country, and once you click on the link, the email owner is asked to provide certain personal or financial information like credit card numbers, national ID, passport numbers, etc. In addition to other important personal data. He may also be asked for even a small money transfer in order to receive the prize. This puts personal information at risk and increases the chances of money being stolen from private accounts.

Among the more deceitful and cunning methods of online fraud is the act of sending a fabricated email that appears to originate from a friend or an official entity, whereas it's just a phishing attempt. This falsely requests specific and sensitive information. For example, the message may inform you of a need to change your PayPal password due to an attempt to breach it, appearing to be from the official website, increasing the likelihood of executing the required action by entering a new password, allowing scammers to use it to steal money [(1).]

The smartphone and tablet devices:

Installing pirated (hacked) or unidentified applications, as well as clicking on links from unknown source, leads to the compromise of personal data such as images and files, as well as the theft of sensitive

[1] What is email fraud? Cloudflare. On site: https://cutt.us/mg8Sf

information such as passwords and bank card numbers, which leads to a person falling victim to cybercriminals and being blackmailed for payment of money or misuse their private data can also occur through impersonation, where an online friend's identity, name, and profile picture are mimicked to request a service, like transferring money to a phone number or using personal information.[1]

Computer

Some computers owned by both large and small companies and institutions contain extremely important information, Therefore hackers and scammers resort to hacking the computer using malicious software and links, causing shutdowns, Then, they contact the owners of these companies and institutions to extort money from them in return for restoring access to their accounts to retrieve the stored information.[2]

E- Commerce

With the growth of the size and prestige of e-commerce, a new form of online fraud has emerged that targets victims from customers on the websites of shops, that is, users can visit a fake website intending to purchase goods, only to become victims of scams and online fraud [3], which means that he will pay money without getting anything in return. Some fake websites may redirect users to unknown electronic payment methods, in order to steal banking information.

Exploiting Disasters:

During crises such as natural or health disasters like the "COVID-19 pandemic," cybercriminals organizing deceptive campaigns soliciting donations to aid victims. This deceit tricks individuals into disclosing private banking information, a clear instance of online fraud.

[1] Mobile phone fraud, Action Fraud - National Fraud&Cyber Crime Reporting Centre. On site: https://cutt.us/1FoJG

[2] Computer and Internet Fraud, Impact Law. On site: https://cutt.us/DtS4E

[3] Varga, Gergo. 7 Types of Ecommerce Fraud & How to Detect Them, SEON. On site: https://cutt.us/TvLAe

Chapter Two

How to Carry Out Online Frauds

- First: Loopholes that help with Online Frauds
- Second: Personal Data Security and Online Fraud
- Third: Digital Footprint and Online Fraud

02

First: Loopholes that help with Online Frauds

Digital loopholes are one of the factors helping to fall victim to online fraud, and a digital vulnerability is defined as term used for weak spots within computer operating systems. These weak spots can be exploited to penetrate the operating system, leading to modifications that could permanently destroy it or enable spying on the information of the breached computer, or what is known as the victim's device[1]; security vulnerabilities can also be found in all software, not only in operating systems. They stem from programming errors committed by developers and pose a security threat due to their frequent lack of detection, often necessitating a new release to find a solution. These vulnerabilities are commonly known as "Zero-day vulnerabilities" that hackers always use in their cybercrimes. The Zero-day vulnerability is one of these flaws, which is a software vulnerability that unauthorized intruders can exploit, as Software developers are often unaware of these weaknesses or fail to develop fixes for them resulting in a serious breach of cybersecurity[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://cutt.us/FXNvU

How Zero-Day loophole attack works

The operation of Zero-day vulnerabilities is often carried out in accordance with several sequential and consecutive stages. The following is an explanation of these stages based on their logical and procedural sequence:

Searching for security vulnerabilities:

This is the initial step where attackers search for security vulnerabilities by examining the software code or testing common applications. They may also acquire weaknesses from the black market[1].

Creating Exploitation Code:

Attackers create malware or other technical means to exploit the identified security vulnerability.

Identifying Affected Systems with the Security Bug:

Attackers might employ bots, automated scanners and other methods to identify systems that suffer from the security bug.

Planning for the attack:

In a targeted attack on specific individuals or organizations, attackers conduct a detailed reconnaissance to identify the best method to breach the vulnerable system. In non-targeted attacks, attackers often use bots or massive phishing campaigns to try to penetrate as many vulnerable systems as possible.

Infiltration:

An attacker penetrates the devices of individuals or organizations.

Launch of the Zero-Day Zero-day loophole:

Following the preceding steps, the attacker begins remotely executing the software instructions on the compromised device.

[1] How to Handle Zero-day, Nordic Defender, 2022. On site: https://cutt.us/gUQ7g

Examples of Zero-Day attacks

The following is an example of vulnerability attacks that reveal the risks of such attacks to organizations and individuals.

Sony:

In 2014, a Zero-Day attack targeted Sony Pictures, , resulting in the destruction of Sony's internal network and the leakage of sensitive company data on file-sharing sites, including personal information about Sony employees and their families, internal correspondence, information about executives ' salaries, and copies of unreleased Sony movies.in this attack, the attackers used a different types of malware to wipe multiple systems on Sony's network[1].

The WannaCry attack:

This attack caused the disruption of over 200,000 devices in one day all over the world in May 2017. The ransomware attack spread through computers running Microsoft Windows operating system, taking control of users' files and demanding a ransom in Bitcoin for their release. The reason behind this attack was the continued use of outdated computer systems that were not updated.

The cybercriminals responsible for the attack exploited a vulnerability in the Microsoft Windows operating system an intrusion technique known as EternalBlue.

Microsoft had issued a security patch two months prior to the attack to protect users 'systems, but as many individuals did not regularly update their operating systems, they were the primary targets in this attack. The intruders initially demanded a ransom of $300 in digital Bitcoin, later raising it to $600 per individual for file retrieval.[2]

Non-targeted attacks of Zero-Day loophole

It is necessary to mention here a type that is extremely important for us as individuals; Non-targeted zero-day attacks are commonly launched against a large number of home users (ordinary individuals) who use a vulnerable system, such as an operating system or browser. The attacker's primary aim is often to breach these systems and utilize them to build extensive botnets for executing larger cybercrimes later.[3]

1. VB2018 paper: Since the hacking of Sony Pictures, Minseok (Jacky) Cha, AhnLab, South Korea. On site: https://cutt.us/ZwCye
2. What was the WannaCry ransomware attack? cloudflare. On site: https://cutt.us/8jM6q
3. Zero Day Exploit: All You Need to Know, phoenixnap, 2023. On site: https://cutt.us/Tr7jJ

Second: Personal Data Security and Online Fraud

Information security

Refers to a set of security measures and tools that widely protect sensitive information from misuse, unauthorized access, or Disruption or destruction. Information security includes physical and environmental security, access control, and cybersecurity [1].

Data theft

It is the act of stealing digital information stored on computers or mobile devices to obtain confidential information or violate privacy, such as bank account details, internet passwords, passport number, medical records, online subscriptions, etc.

And so on. Once an unauthorized person has access to personal information, he can delete, change or block access to it without the owner's permission[2].

Data theft usually occurs due to individuals' desires to sell information or use it for identity theft. If data thieves manage to steal enough information, they can use it to access secure accounts, or issue credit cards using the victim's name, or otherwise use the victim's identity for their own benefit; we point out here that the word "theft" In the realm of the internet world does not literally mean taking information away from the victim or removing it, Instead, data theft involves the attacker simply copying the information for their own use. This cybercrime is commonly referred to as "data breach" or "data leakage."

The most common form of this type of crime is phishing, and it occurs when a fraudster disguises himself as a trusted entity to deceive the victim into opening an email, text message or instant message containing malicious software, and people who fall victim to phishing attacks are exposed to identity theft.

People can also cause themselves to be exposed to cyber fraud by downloading programs or data from hacked websites infected with viruses such as worms or malware, which gives criminals unauthorized access to their devices; and allows them to steal data.

[1] What is information security? Microsoft, available at the link.

[2] What is meant by data theft? And how can it be prevented? available at the link.

Third: Digital Footprint and Online Fraud

The term “Digital footprint” or “Digital shadow”, Refers to the trail of data that you leave when using the internet, and it includes the websites you visit, the emails you send and receive, and the information you provide online[1].

A digital (or electronic) footprint can be used to track anyone’s activities online and on their devices For instance, actions like social media posting, subscribing to newsletters, leaving reviews online, or shopping online all contribute to the “Digital footprint; websites can track visitors’ activities by installing cookies on their device, and applications can also collect users ‘ data without their knowledge; Merely granting access to an organization to your information can enable them to sell or share your data with third parties. The worst scenario is the potential exposure of the confidentiality of your personal information within a data breach context.

[1] What is a digital footprint? And how to protect it from hackers, Kaspersky. On site: https://cutt.us/teSUS

Types of digital footprint

There are two types of digital footprint; active and inactive, here's an explanation of both types:

Active Digital Footprints:

It is intended for the user to intentionally share information about himself, for example by posting or sharing on social platforms or internet forums. Alternatively, if a user logs into a website with a username or registered profile, any posts he publish become part of their active digital footprint.

Activities like online form submissions, subscribing to newsletters, or agreeing to accept cookies in your browser all contribute to an individual's active digital footprint.

Inactive (passive) digital footprints

An inactive digital footprint is created when information about a user is collected without their awareness. For example, This occurs, when websites collect information about how many times a user has visited, the where they enter from, or their IP address.

Users may not realize this hidden process is happening. These footprints can also be shaped by internet browsing habits, social media interests, search queries that shape your profile, and advertisers who leverage likes, shares, and comments to build impressions of your personal interests, for targeted content [1].

[1] Hammadi, Khaled. The digital fingerprint... the hidden electronic shadow, Larbi Tebessi University, Tebessa, Algeria, July 2021 AD, available at the link: https://cutt.us/QToSN

Negative Effects of Digital Footprints

Digital footprints can lead to damages and negative consequences for internet users. These damages don't occur unless there are errors on the part of the user. Here is an explanation of the most significant negative effects that digital footprints can cause:

01

They are relatively permanent data, becoming available for public or partial access, such as with Facebook posts and other social applications, weakening the owner's control over how others use it.

02

The digital footprint shapes individuals' online reputations, similar to what occurs in real life.

03

Words and images published or altered by an individual online can be misinterpreted, causing unintended offense

04

Content intended for a specific group can spread beyond it, potentially damaging relationships between individuals.

05

Cybercriminals can exploit your digital footprint for purposes such as identity theft, accessing accounts, or creating fake identities using your personal data to deceive others

Examples of Digital Footprint

An internet user can leave behind digital footprints through any activity they engage on the internet.

Here are some examples of such activities:

01 Online shopping.

02 Purchases from e-commerce sites.

03 Register to create an account on a specific website.

04 Downloading and using applications.

05 Signing up for newsletters from brands.

06 Online banking services.

07 Use the mobile banking application.

08 Subscribing to printed or online publications and blogs.

09

Open a credit card account.

10

Using social media on your devices.

11

Logging into other websites using social media credentials.

12

Communicating with friends and contacts online.

13

Sharing information, data, and images with acquaintances.

14

Subscribing to online news sources.

15

Re-sharing information that you read.

16

Using fitness tracking devices.

Digital Footprint protection

Here are some tips to safeguard personal data and manage personal reputation online:

Verification of Digital Footprint through search engines

By entering their name in search engines, an individual can review the search engine results and available information about them for public access. If any of the results display the individual in negative appearance, they can reach out to the site administrator to inquire if the content can be removed setting up Google Alerts is one way to monitor the username[1]

Reducing the number of information sources

Websites often contain more information than an individual might want to display. These sites frequently include personal information, such as phone number, address, and age, Therefore individual should consider removing personal information from these websites whenever possible.

Restricting the amount of shared data

Every time we provide personal information to an organization, we are creating our digital footprint, increasing the likelihood that the institution storing our data might misuse it or expose it to breaches, putting our data at risk. Therefore, we need to think carefully before providing any information to any entity online

Checking the Privacy Settings

Privacy settings on social media allow you to control over who can see our posts. Therefore, it is advisable to review these settings, and make sure that they are set to the level that suits us. For example, Facebook allows post restrictions, and the creation of custom lists for individuals allowed to view specific posts

Think carefully before sharing our information on social media

Social media facilitates connecting with others, but it can also make it easier to over-share personal information on it, Therefore, it's essential to think carefully before disclosing our location or any other personal information, such as phone numbers or email addresses.

[1] How to protect your digital footprint, state farm, 2023. On site: https://cutt.us/OcHUG

Avoid unsafe sites

Every time we access the internet, we must ensure that we are dealing with a secure website whose URL starts with https:// instead of http:// -, where the letter "S" stands for secure." Additionally there should also be a lock symbol to the left side of the address bar.

Caution when using a public Wi-Fi network

Public Wi-Fi network is inherently less secure than private network, because it's uncertain who set it up or who might be observing it. Therefore, it's advisable to avoid sending personal information when using public Wi-Fi networks.

Delete old accounts

One ways to reduce our digital footprint on the internet is to delete old accounts, such as old profiles on social media that we no longer use or newsletter subscriptions..

Create strong passwords and use Password Manager

A strong password should be long, that is, consisting of at least 12 characters, preferably more, including a mix of uppercase and lowercase letters, symbols and numbers. The more complex and challenging the password, the harder it is to breach.

Using a Password Manager helps in creating, storing, and managing all our passwords securely in one online account.

Avoid logging in using Facebook credentials

Logging into websites and apps using Facebook is convenient. However, every time we use our Facebook credentials to log in to an external site, we grant permission to the company to access and retain our personal data, potentially risking our personal information.

Regularly update software

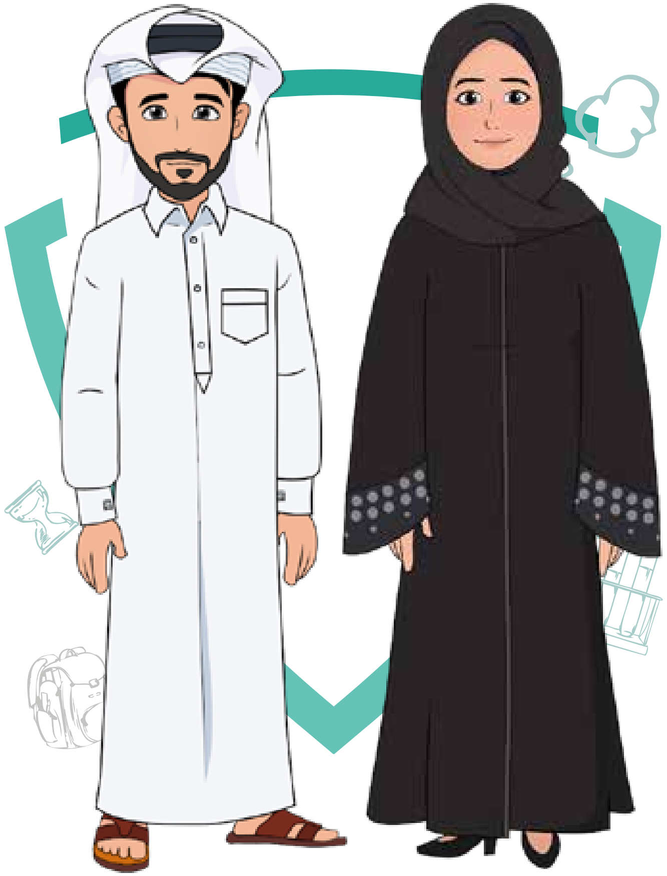
Outdated software might contain a wealth of digital footprints. Without the latest updates, cybercriminals can access to this information easily. Cybercriminals can easily exploit software vulnerabilities to access the victim's devices and data. The solution lies in consistently updating software, as older programs are more susceptible to infiltrator attacks.

Set a password for your mobile phone

Set a passcode for your mobile device to prevent unauthorized access it if it's lost. When installing an application, read the user agreement, because many apps disclose what kind of information they collect, and what it might be used for. Some apps store personal data, such as e-mail, location and online activities.

Act quickly after a data breach

In case of suspected data breaches, especially those involving financial loss, immediate action is crucial. Start by changing any compromised passwords. If you've used the same password for other accounts, update it across all accounts[1].

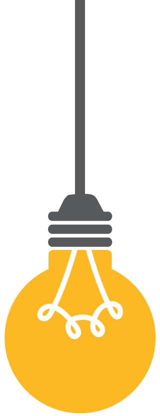


[1] How to Map, Monitor and Manage Your Digital Footprint, Bitdefender. On site: https://cutt.us/G7awc

Chapter Three

How to React When Exposed to Online Fraud

- First: Guidelines for protecting against online fraud
- Second: Data protection against online fraud
- Third: Authorities I turn to when exposed to online fraud



03

First: Guidelines for protecting against online fraud

Fraudsters create new methods and mechanisms to carry out their cybercrimes, but taking some simple measures can enhance information security, and here are the most important ones:

Downloading applications from well-known app stores.

All applications should be downloaded from well-known stores, as the process of downloading any application from unknown sources might expose your data and privacy to theft, which could lead to various forms of online extortion and fraud.

Updating phone applications

Installing the latest updates for your phone is essential, as they always contain files that reinforce the phone's protection against various forms of hacking.

Avoiding unknown source links

Even if sent from friends, clicking on these links can make you vulnerable to hacking or installing malicious software on your phone without your knowledge. Similarly, do not open unknown email messages.

Be cautious about transactions involving unknown parties.

Be cautious when asked to receive any financial transfers and then transfer them to a third party, as this could be a scam or money laundering operation.

Employing anti-virus software

Whether on a smartphone or a computer, installing reputable antivirus software is important to enhance device protection.

Use complex passwords and change it occasionally

It's preferable for passwords to include letters, symbols and numbers, and they should be changed immediately if any suspicion arises

Refraining from shopping on unfamiliar websites.

Only make online purchases from well-known sites and reputable online stores, and if there are doubts about a website's credibility, it's essential to research it further to ensure its reliability.

Second: Data protection against online fraud

Protecting personal and financial data from fraud is possible, and can be achieved by several measures. Here are the most important ones:

- Be vigilant for frauds when dealing with intrusive communications by people or any entity; whether through phone calls, mail, emails, or on social media sites, as they could be a fraudulent operation.
- If you've only met someone online, take the time to do additional research about them, such as using Google Image search for their photos or searching for other individuals who may have interacted with them.
- Do not open suspicious texts, pop-up windows, or emails; ensure the caller's identity through an independent source, like searching online.
- Secure your personal details, such as putting a lock on your mailbox, keeping your passwords and PIN numbers in a safe place, and be cautious about sharing personal information on social media.
- Constantly updating operating systems, and maintaining a backup copy of content.
- Secure your Wi-Fi network with a password and avoid using public computers or WiFi hotspots.
- Review your privacy and security settings on social media platforms.
- Be cautious about any requests for your details or money.
- Be careful when shopping online, especially with overly enticing offers.
- When reviewing a new profile, note anything unusual about the other person, such as images, location, interests, or linguistic skills matching their background. Scammers often use forged images found online. Conduct a search for the person's image to verify their identity. You can use image search services like Google.

- Change your passwords on the internet if you suspect your computer or phone has been hacked, you should perform a comprehensive system check using reputable antivirus software, and then change your password immediately. The same applies to online accounts, whether on social media platforms or shopping websites – change your password immediately.
- Bookmark essential websites you frequently visit, and only open them from there to avoid accidentally opening fake pages.
- There are several warning signs for detecting forged documents such as bank account data or flight itineraries, which might be traps set by intruders in the form of fake gifts to obtain personal information from individuals. Look for signs like generic greetings instead of personalized ones, use of nonexistent organizations, formalities, weak grammar, and spelling.
- Remember that legitimate error messages from Microsoft or other major tech companies will never include phone numbers for you to call.
- Remember: Microsoft and other legitimate tech companies will never call you to inform you of a problem with your device. Unless you contact them first, technical support agents will never need Social Security number or any unrelated personal information. If you receive an unwanted technical support call, end the call.
- If your screen suddenly fills with scary pop-ups windows, immediately shut down your computer (try pressing ALT+F4 if you can't do this with the mouse), and if you can't close the browser, try restarting the computer[1]

[1] Protect yourself from online fraud and attacks, Microsoft. Available at: https://cutt.us/YVxY1

Third: Authorities I turn to when exposed to online fraud

In case of exposure to an online fraud crime, it’s crucial not to leave the matter unattended but to act promptly to prevent the situation from worsening. First: Do not engage with the scammer or resend any messages that doubt their credibility again, then: Close all active accounts upon receiving a warning message or if you suspect any of your accounts have been compromised, or upon receiving a threatening and extortionate message from an unknown source. Also, turn off the devices. while retain the message sent, as it serves as evidence incriminating the intruder, Here you have to inform a to a trusted individual, such as parents or a school authority, this is a necessary step that should not be overlooked. According to global statistics, one out of every 100 people is subject to internet crimes, with forgery and fraud being at the forefront.

Moreover, Do not comply with the intruder; they are skilled at intimidating others. Do not succumb to their demands, such as sending money, as happens in ransomware attacks, and do not believe what the intruder says and do not let them manipulate your emotions.

Finally, Provide any information or specific details about the intruder or any messages received to trusted individuals who can then pass it on to the appropriate law enforcement authorities responsible for combating cybercrimes in your country for your protection, whether through email or contacting hotlines or numbers dedicated to combating cybercrime.

Examples of the most famous online frauds

The method of gaining the victim's trust, and then proceeding to steal their money and personal data is the most widespread in phishing attacks. Here hackers deliberately launch their attacks through malware (malicious software), and online fraud attacks often end with severe consequences for individuals and companies.

In order to understand the danger of online fraud, we present some of the most notable examples that have occurred worldwide

First Example: Toyota Boshoku Company

In 2019, "Toyota Boshoku," a company involved in supplying Toyota cars and providing some equipment, fell victim to an online fraud operation amounting to approximately 37 million USD. Online fraudsters convinced the company's financial director to change the recipient's bank account information, enabling them to obtain these funds. [1]

Second Example: Digital Currencies

In 2017, many people lost thousands of dollars after losing digital currencies, specifically "Ethereum." Hackers breached the currency wallets and transferred them to their own servers. Also in the same year (2017), the "WannaCry" virus, a ransomware attack, disrupted computers. To regain access, the hackers demanded a sum of money in Bitcoin to avoid detection and escape punishment. [2]

1. Toyota Boshoku Corporation loses $37 million in Business Email Compromise scam, CYWARE SOCIAL. On site: https://cutt.us/fFDMv
2. Ransomware News, Ransomware Timeline: Top Stories December 2017, Cyber defense magazine. On site: https://cutt.us/IJBEQ

Third Example: Yahoo Inc.

During the period between 2013 and 2016, Yahoo suffered a data breach affecting about 3 billion users. The intruders gained access to information and passwords that could be used to access other online services and accounts. [1]

Fourth Example: Money Theft in Russia

In Russia between 2013 and 2014, one of the most prominent online fraud methods, where a fraudster contacts his victim, impersonates an employee of the target's bank, and asks him for information related to the debit card, under the pretext of stopping suspicious financial transactions. After obtaining the card information, the fraudster used it to steal and transfer funds to their accounts.[2]

Fifth Example: $600 Million Theft in a Massive Cryptocurrency Fraud Operation

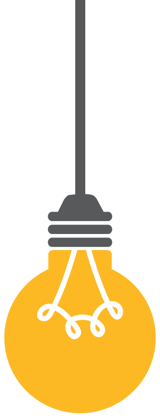
Cyber pirates stole approximately 600 million dollars, marking one of the biggest fraud operations in the history of digital currencies. They exploited a security flaw in the currency system to pilfer funds belonging to tens of thousands of cryptocurrency community members.[3]

[1] All 3 Billion Yahoo Accounts Were Affected by 2013 Attack, The New York times. On site: https://cutt.us/oOhv7

[2] . The most famous online fraud methods that have spread in recent years, Russia Today, 2020 AD. Available at: https://cutt.us/gDg5J

[3] . Online piracy: $600 million have been stolen in a massive digital currency fraud, BBC Arabic, 2021 AD. Available at: https://cutt.us/ToS7P

Exercises and training



Exercises and training

Exercises are a major part of the training process, and they achieve several goals and aims, as follow:

- Exercises are an effective tool to assess students' utilization of the training content and its impact on their cognitive inventory.
- They serve as a vital means to reinforce information and knowledge, constituting a rapid review of the training content
- They help to identify knowledge gaps among students.
- They act as a form of feedback for the trainer, providing information on the effectiveness of the training kit and the training method.

Approach to Dealing with Exercises:

The exercises mentioned in this section are comprehensive of the training content in this kit, here's an outline of the proposed methodology for dealing with them:

- During the training, after introducing an idea, the trainer will request students to open their respective booklet and answer the specific question, directly related to the presented idea or subject
- The exercises are carefully selected to be simple, easily understood, and solvable by middle school students. The trainer may offer support to students in answering some exercises if necessary, at their discretion.
- The exercises are divided into two parts; one for in-classroom use, called classroom exercises, and another is non-classroom, to be completed at home by the students.
- The answers for each exercise are provided, highlighted in a different color.

Below is an explanation of exercises specific to Middle school students, arranged according to chapters and classified as in-classroom and homework exercises

(Non-classroom Exercises). These exercises, in the form presented here, are the same as those in the students' booklet.

pay attention!

Online fraud

A type of deception and tricks carried out over the internet, often occurring in chat rooms, via e-mail, on forums or websites (the web). The goal of these crimes is to defraud customers and users by stealing money, important personal information, and other purposes.

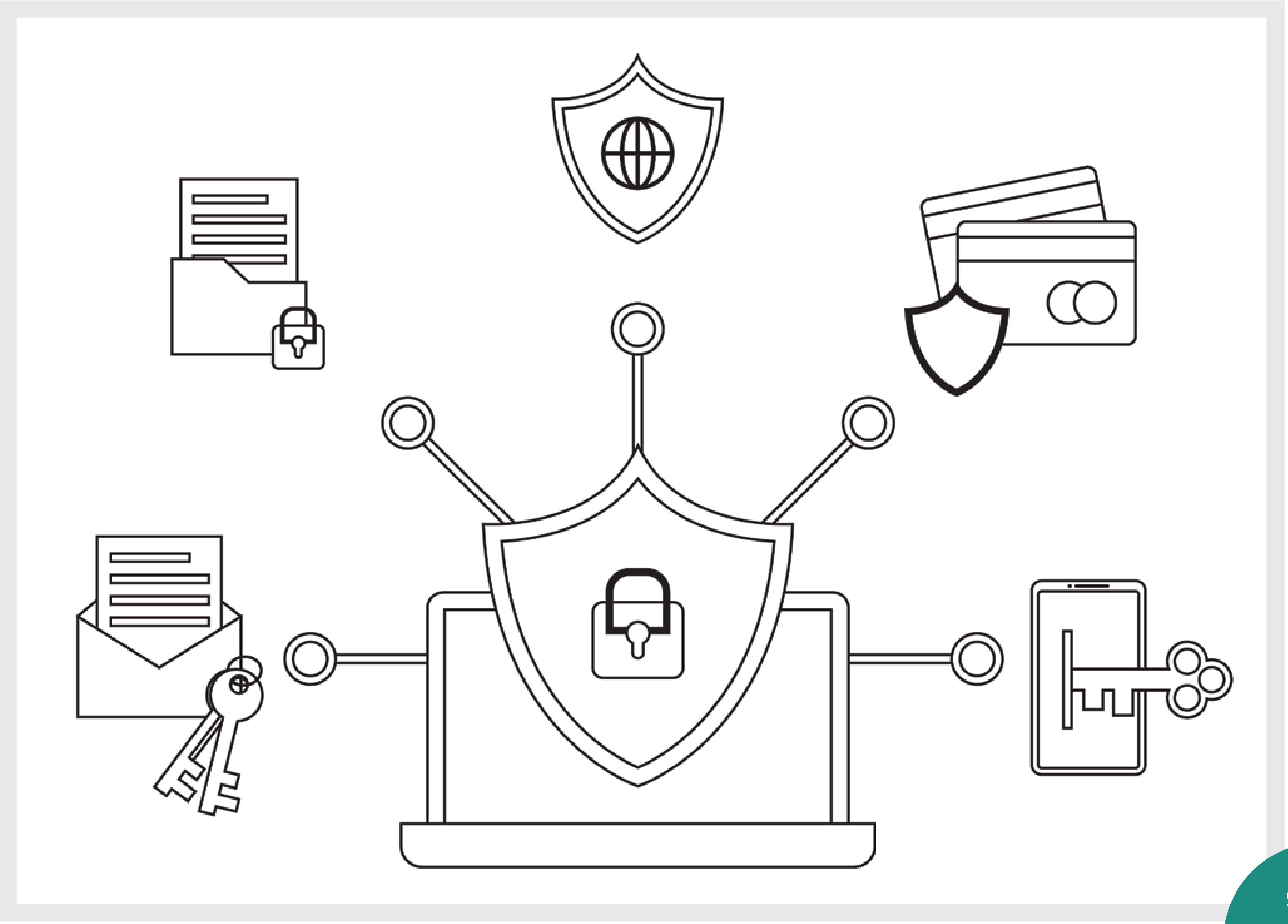
First:

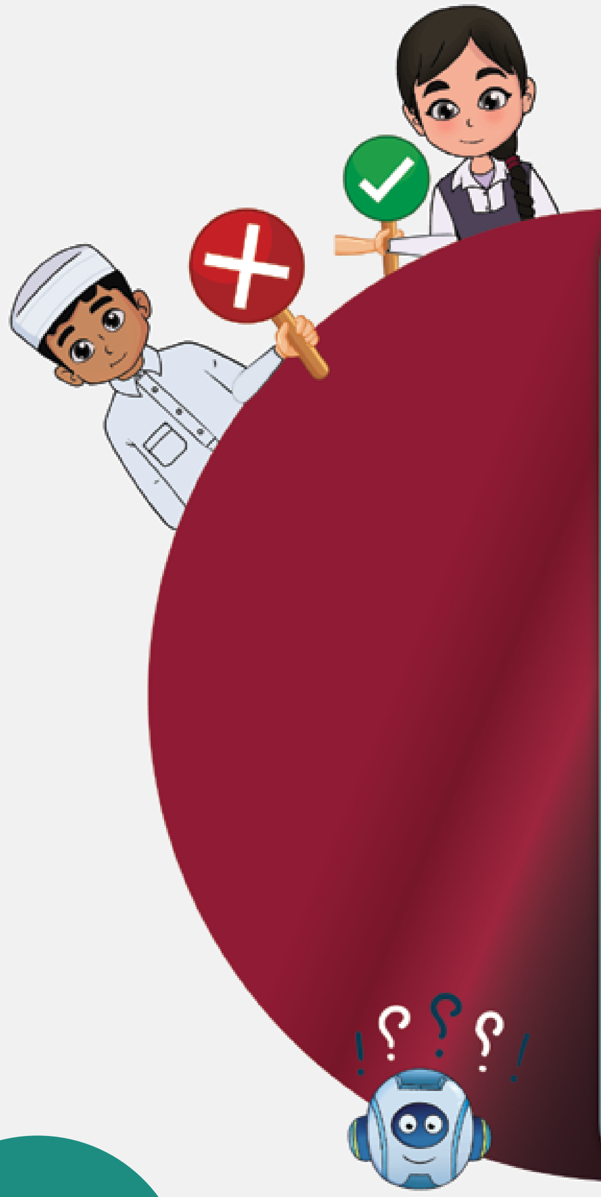
in-classroom Exercises

The exercises here are accompanied by the answers, while in the student's booklet they are written without a solution, and are accompanied by guidance for the student on how to solve, when necessary.

Do you know that...?

The majority of prizes and gifts received online for no reason are the beginning of an online fraud process.





Exercise 1

Mark (✓) next to the correct statement,

and (✗) next to the incorrect statement

1 Online fraud is a deliberate manipulation of information and data on the computer. ✓

2 Online fraud is the authorized access in order to obtain information and data on the computer. ✗

3 Unauthorized access to devices or systems to gain illegal profit or cause harm is a type of online fraud. ✓

4 Modern technology assists online fraud perpetrators in committing crimes only on a local scale. ✗

5 Online fraud is the use of authorized systems and devices to deceive others. ✗

6 Information fraud involves cheating and deceiving by manipulating information processing systems unjustly, to obtain services, money, or assets. ✓

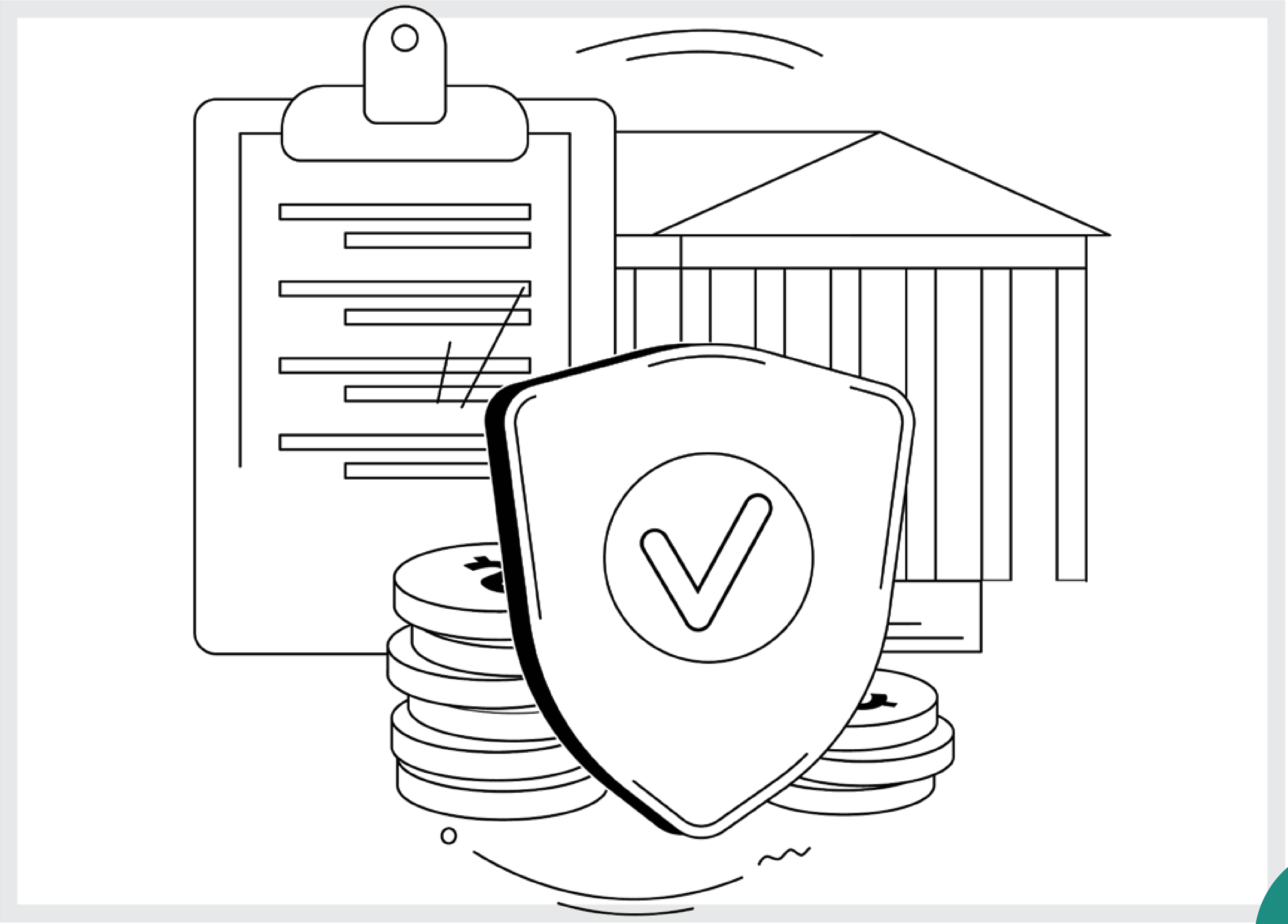
7 Online fraud is gaining money through illegal means only from outside the country. ✗

8 Criminals in online fraud use technologies in a legitimate way and without any manipulation. ✗

pay attention!

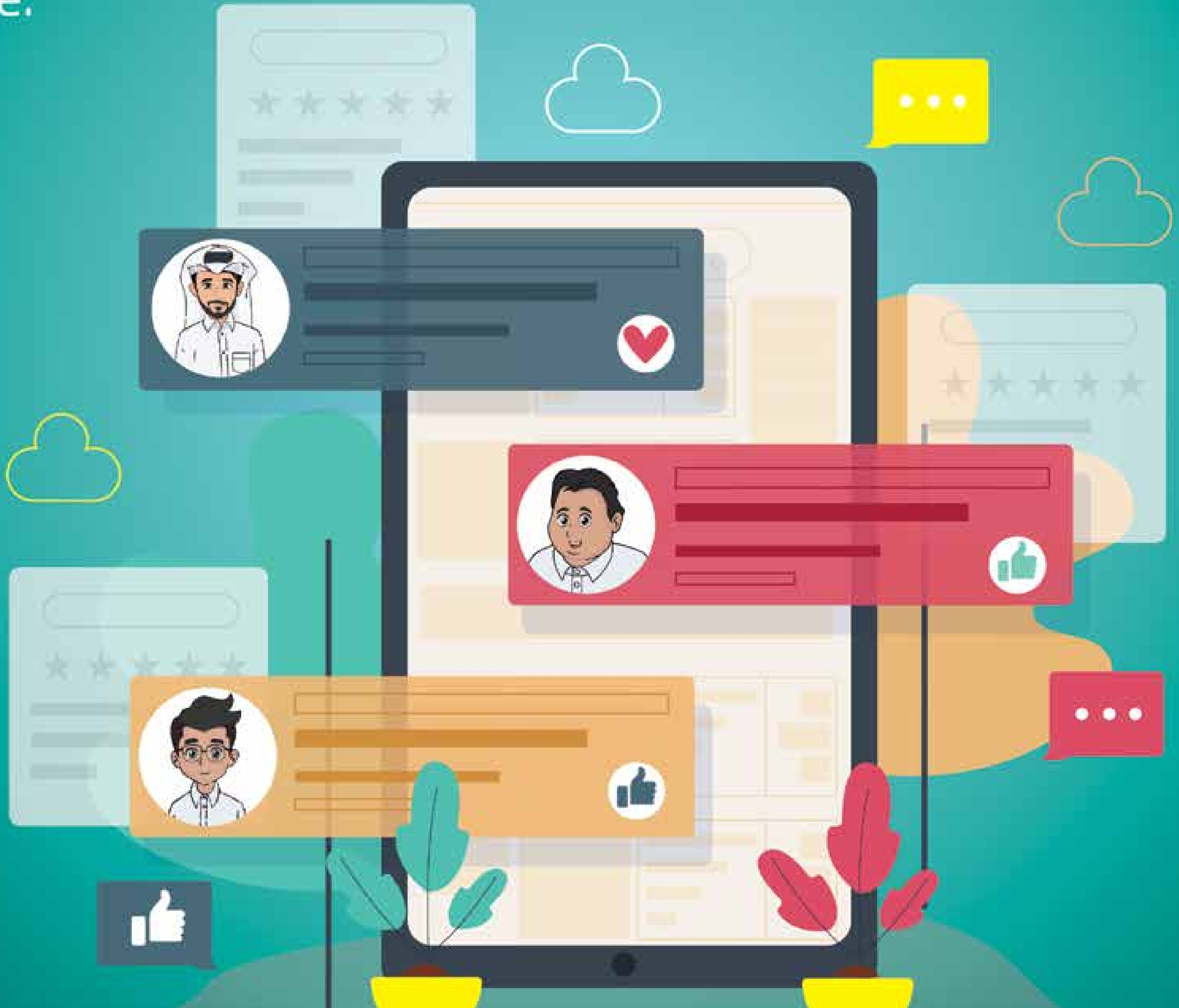
Cyber Fraud

Seizing others' money through deceitful means, often involving the use of computers.



Do you know that...?

Your digital footprint defines your online reputation, much like in real life.



Exercise 2

Match the terms from column (A) with their corresponding from column (B):

Column (A)

- SMS fraud ○
- Ad fraud ○
- Ransomware viruses ○
- Traditional online fraud ○
- Voice fraud ○
- Online shopping fraud ○
- Fundraising fraud ○
- Shopping fraud ○

Column (B)

- ● A link is sent via text message, and once clicked, the fraud is initiated.
- ● Malicious ads loaded with viruses are used to steal information and data.
- ● A type of cyber fraud in which the victim is threatened with data destruction or payment of a ransom.
- ● It involves purchasing credit card data and using it to buy products online.
- ● It relies on deceiving others through voice alteration software to convince victims to share personal data and information.
- ● It deceives the seller into thinking that the buyer has made the payment, but after sending the product, the money is not added to their balance.
- ● It exploits fake charitable organizations' names to obtain money by eliciting sympathy from others.
- ● It occurs during the victim's shopping experience, where after paying for a product, they either receive nothing, or they might receive a wrong or counterfeit product.

Exercise 3

Complete the sentences with the appropriate words:

1 Identity theft is considered the most dangerous form of online fraud; where the criminal steals personal ...**data**..., such as name, date of ...**birth**..., address,**banking** account details, and all other important information.

2 This information is used to steal ......**money**...... and the identity can be exploited to open a bank...**accounts**... obtain ......**credit**...... cards or loans, or to register ......**phone**...... lines.

3 Online fraud criminals can steal personal ......**data**...... to take over existing bank ... accounts...**accounts**... of the person by using their personal ......**data**......

4 It is essential to avoid giving any personal ......**data**...... to others, and you must delete any document or file containing confidentia **information** or ......**credit**...... card numbers before disposing of it.

5 Ask your bank to send you a notification or ....**contact**....... you in case there is any suspicion of unusual or unauthorized transaction on your bank ....**account**.......

6 You must be very careful in your dealings with commercial ...**websites**...... , or with others, whether through the phone or ...**credit card** , or the Internet in general, especially ..**social media**... platforms.

7 Avoid opening any suspicious .....**websites**... , and disable pop-up ......**windows**.. Ensure the authenticity of the **information** of the person you are communicating with online.

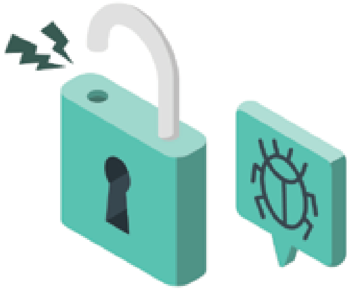
8 Use a strong ....**password**............for your phone and personal accounts, do not share it with others,and remember to keep ...**a backup**...of your data. Avoid using public.....**Wi-Fi**.....networks, especially when accessing any banking-related applications.

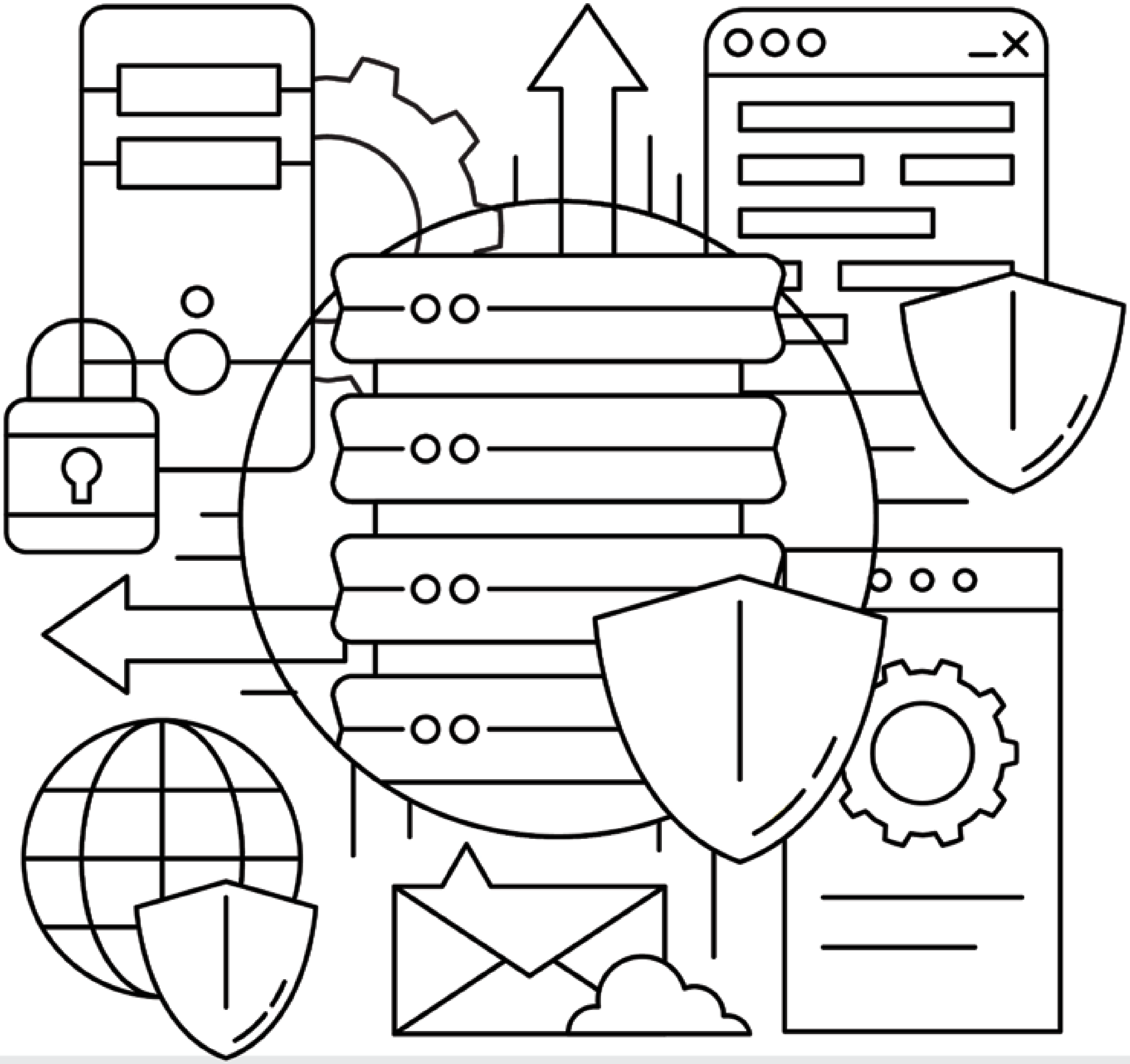
9 If you want to shop ....**online**.......... , you need to make sure that the store is trustworthy, read reviews and ratings from others, and it's better to deal with well-known and secure stores.

pay attention!

Information fraud

Deception or fraudulent manipulation of information processing systems, with the intention of wrongfully gaining access to services, money, or specific assets.





Exercise 4

Put the word (true) or (false) in front of the phrases that are essential for protection against online fraud crimes:

1	It is necessary to use legal versions of banking applications.	True
2	You can download applications from any website.	False
3	You should not disclose your confidential information or personal details during phone calls.	True
4	It's okay to click on any links sent by friends, whether in text messages or through email.	False
5	Using a third party in financial transactions may expose you to fraud or money laundering.	True

6	Using antivirus software is an essential factor in protecting yourself from online fraud.	True
7	You can repeat your name or using your date of birth as a strong password for your accounts and devices.	False
8	You should be careful when shopping online, and it is preferable to deal with well-known websites.	True
9	Writing your banking card details on any electronic shopping application is acceptable.	False
10	Avoid using modified or pirated (hacked) versions of smartphone applications.	True

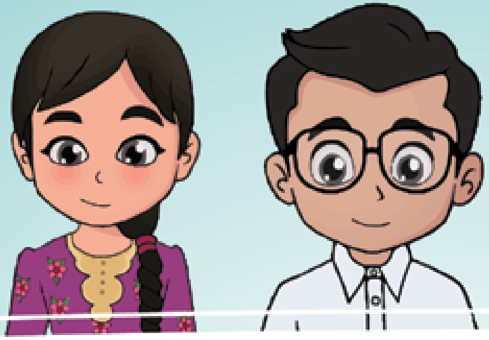
pay attention!

Reasons for falling victim to online fraud

- Lack of awareness about using social media and internet platforms.
- Accessing unsafe websites.
- Sharing personal information on social media and online platforms.
- Dealing with fake online stores.
- Impersonation of well-known personalities such as government employees, experts, executives, or technicians by hackers.
- Exploiting of emotions like during emergencies to attract the sympathy of targeted victims online.

Exercise 5

Place the appropriate word in front of each sentence:



Instructions:

Carefully read the sentences in the table, think of a word or phrase that expresses the meaning of the sentence. And write it in the second column, an example provided below.

- The impact you leave behind and the information you leave behind after each use of the internet.	**Digital footprint**
- Fraud and data theft using technology and the internet.	**Online fraud**
- Programs that help you protect your devices and fend off fraudulent attacks.	**Antivirus software**
- A set of letters, symbols, and numbers used to secure your accounts.	**Password**
- Using an intermediary to transfer money from one party to another.	**Money laundering**

pay attention!

Security Bug

A 'Security Bug' is a term referring to vulnerabilities in computer operating systems and software. These weak points allow attackers to infiltrate the operating system, enabling them to modify it, leading to potential outcomes such as complete destruction, spying on the computer owner's private information, or accessing the victim's device.

pay attention!

The Zero-Day loophole

This type of security vulnerability is present in computer programs and can be exploited by hackers; these security vulnerabilities pose a high level of risk to cybersecurity.

Second:
Non-classroom Exercises

Exercise 1:

Extract the following words from the table:

Instructions:

Carefully read the words listed below and search the table for consecutive letters that form these words. Below is an example for the word "**scam**" and how its letters were found in the table:

h	a	r	m	s	c	a	m	b	n	e	t
i	n	s	t	r	u	c	t	i	o	n	s
r	f	c	h	w	l	h	s	l	o	c	c
i	r	r	t	o	i	a	e	e	r	h	r
g	a	i	t	r	e	r	c	g	d	e	i
h	u	m	p	k	s	m	u	a	e	a	m
t	d	e	d	a	t	a	r	l	r	t	i
p	r	i	v	a	c	y	e	j	s	i	n
d	e	c	e	p	t	i	o	n	n	n	a
b	a	n	k	r	u	p	t	c	y	g	l
m	a	n	i	p	u	l	a	t	i	o	n
t	e	c	h	n	o	l	o	g	y	t	i

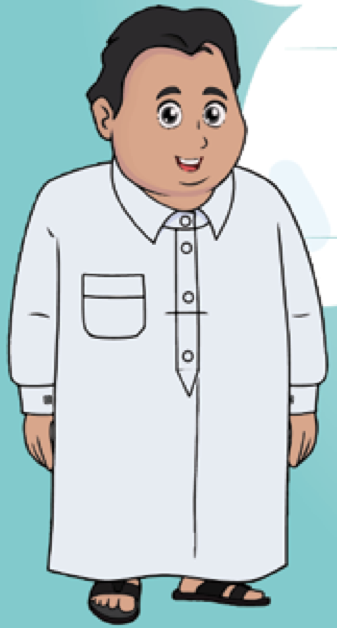
Fraud - Scam - Manipulation - Data - Instructions - Orders - Technology - Harm - Http

Criminal - Crime - Deception - Cheating - Bankruptcy - Right - Work - Privacy - Secure - Legal - Lie - net

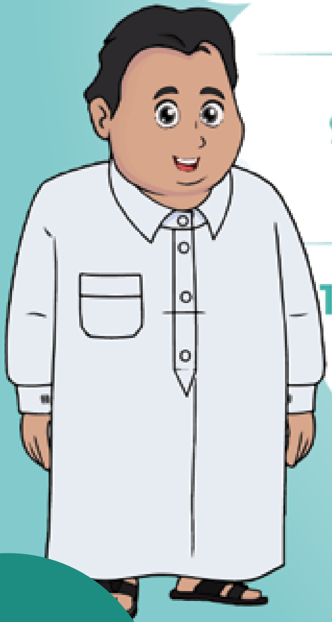
Exercise 2

Determine the correct and incorrect statements:

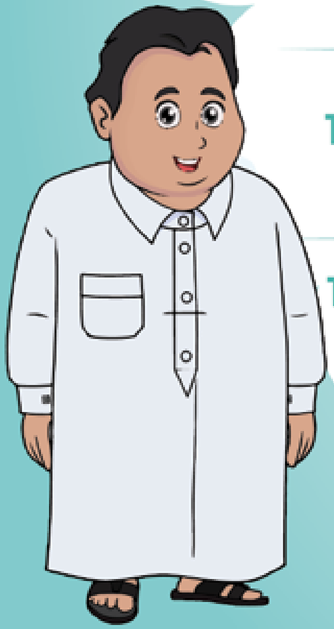
1	Online fraudsters exploit people’s trust to steal their money and data.	Correct
2	Cybercriminals study the victim to know their weaknesses; to gain trust before committing their crime.	Correct
3	Large companies are never exposed to any form of online fraud crimes.	incorrect
4	Online fraud crimes cannot enter into any other areas other than stealing money and data.	incorrect
5	Online fraudsters seek only to obtain money.	incorrect

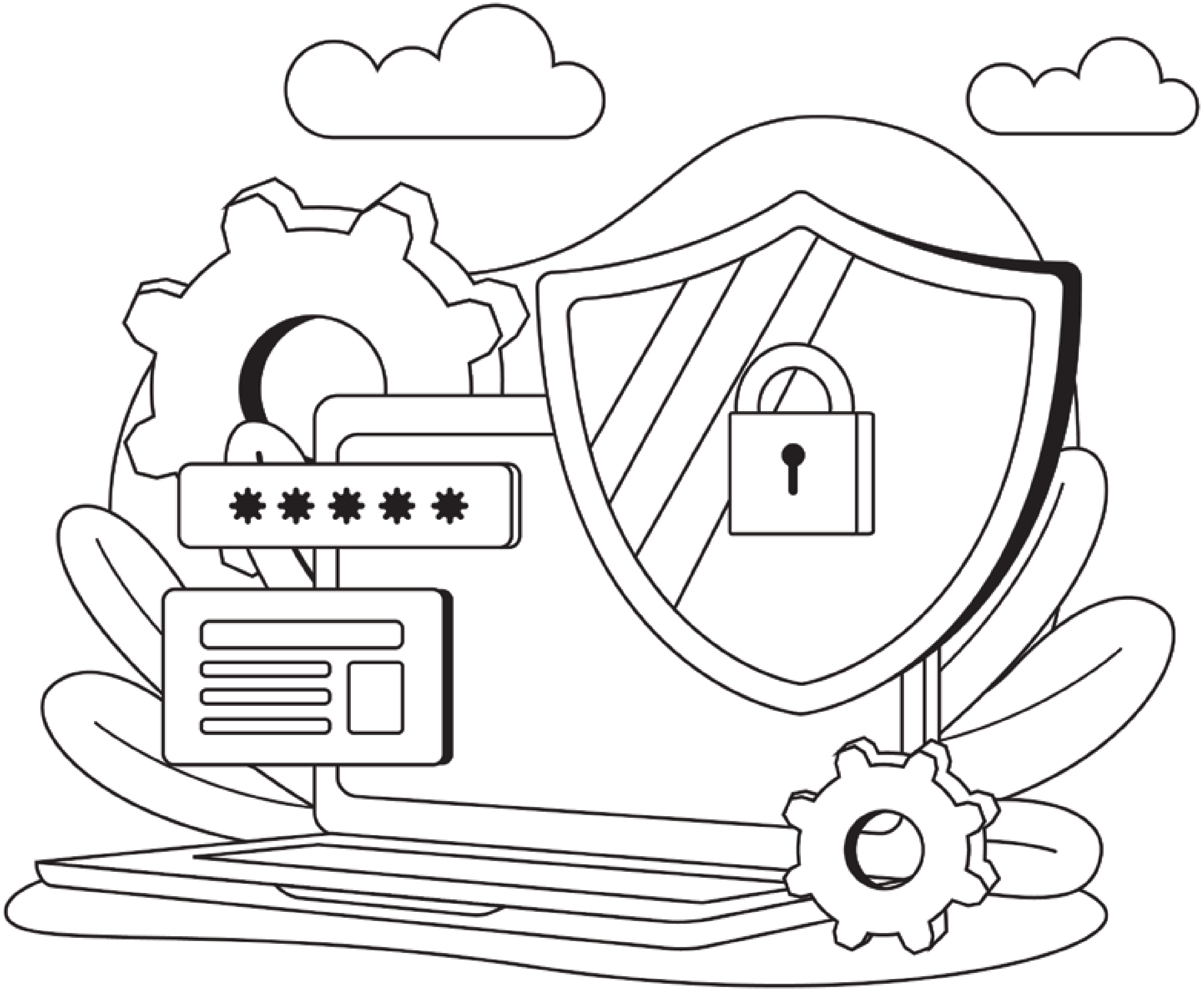


6	Using illegal applications helps online fraudsters.	Correct
7	Applications can be downloaded from any website on the Internet without fear.	incorrect
8	It is okay to share confidential data and information with others over the phone.	incorrect
9	You do not need to use antivirus software.	incorrect
10	Use numbers 1 to 8 as the password for your accounts and devices.	incorrect



11	You can shop from any online store and share your bank card data without fear.	incorrect
12	Fraud cannot occur in the name of charitable or volunteer institutions.	incorrect
13	E-commerce is one of the primary targets of online fraudsters.	Correct
14	Clicking on malicious links without awareness may lead to the theft of your data and accounts .	Correct
15	Ransomware viruses cannot cause any harm to your devices or data.	incorrect





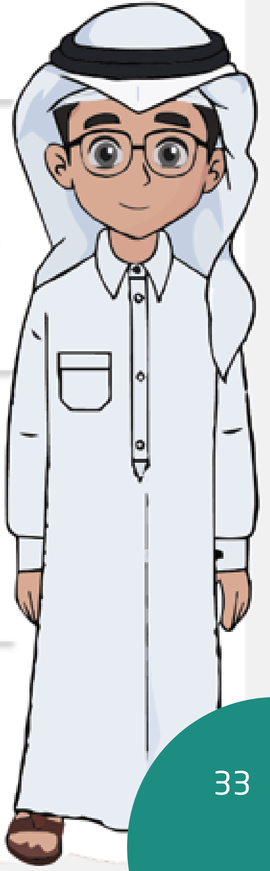
Exercise 3

Complete the following sentences:

1. **Digital footprint**...... is the digital shadow and refers to the trail of data left when using the internet

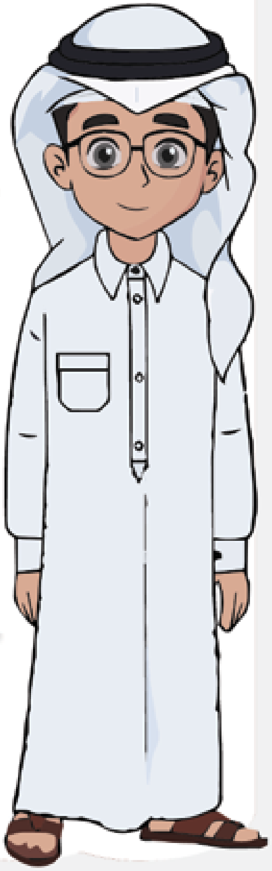
2. Digital footprintɑng includes visits to ...**Websites**......., messages from **chat rooms** and the information you are looking for.

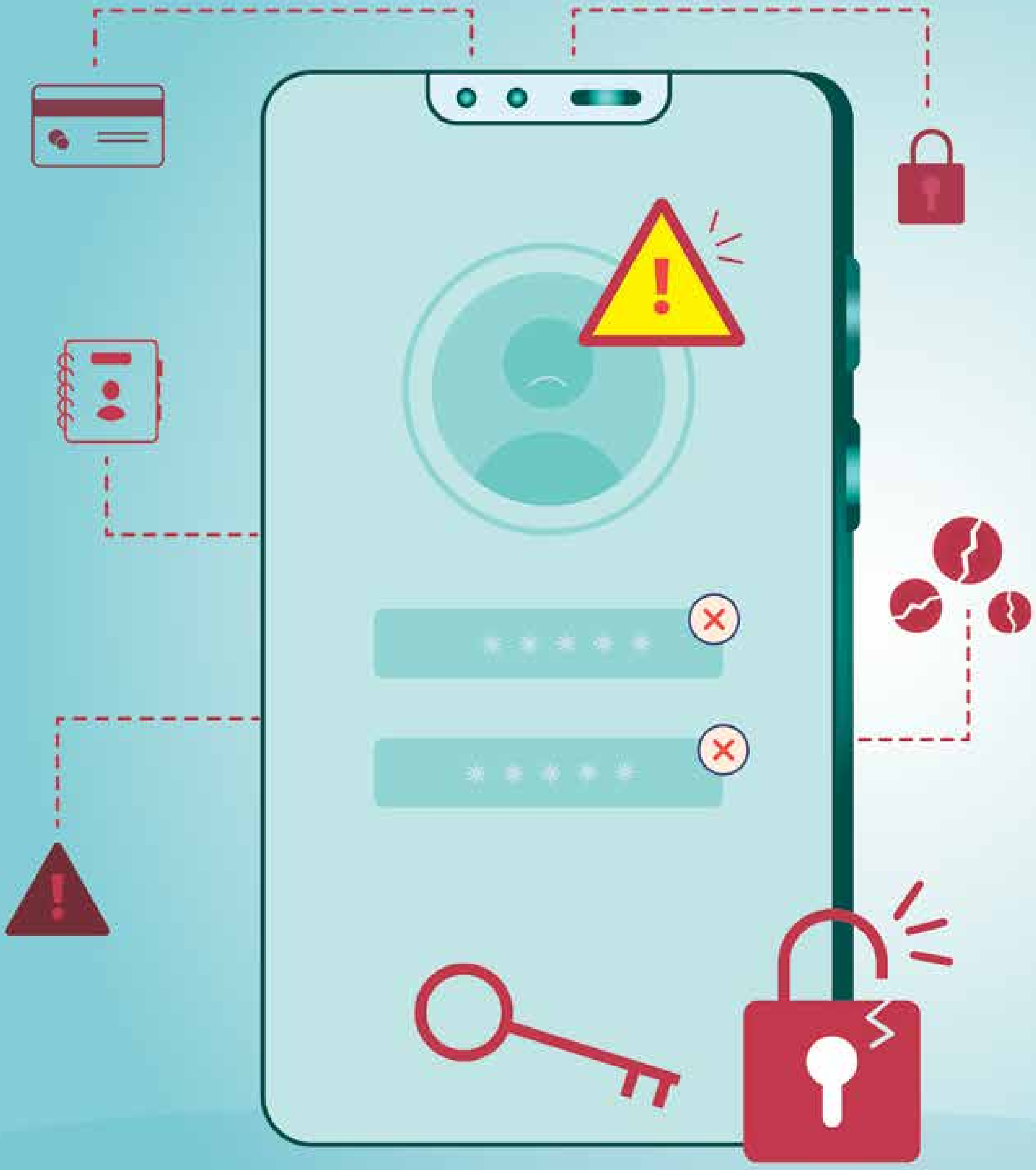
3. The ....**active**........ digital footprint is when you deliberately share information about yourself by participating in ....**Web**.......... sites or forums.



4 The inactive digital footprint occurs through gathering information about the user without their knowledge, either from their website visits or the information they search for and use with their IP address.

5 The digital footprint is very important, especially since it is considered a personal data, and it determines the digital reputation of the person. Some employers resort to tracking the digital Footprint of potential employees and some words or images shared online can be misinterpreted, affecting your reputation or digital Footprint.





Do you know that...?

Using a strong password protects you from online fraud.

Exercise 4

How can you protect yourself from online fraud? Place a word true or false:

1.Downloading legitimate applications from official stores.	True
2.Using modified and leaked versions of mobile phone applications.	False
3.Use anti-virus software and firewalls.	True
4.Sharing personal data on social media platforms.	False
5.Sharing data through phone calls.	False
6.Shopping only from trusted stores.	True
7.Avoid sharing bankcard information on websites.	True
8.It's okay to click on links from unknown sources.	False
9.Be careful of using third-party services during money transfer or withdrawal.	True
10.Choose a strong password consisting of uppercase and lowercase letters, numbers, and some symbols.	True

Exercise 5:

Identify the mistake made by each victim in the following online fraud incidents:

Hamad received an email with a gift of an iPhone 14. So he immediately opened the link provided but found nothing.

If the student highlights the importance of avoiding opening unfamiliar links and stresses the significance of refraining from interacting with unidentified messages offering prizes or gifts, as these messages are often a tactic used in online fraud.

Hala received a message from an international number asking her to send her Facebook account password. Once she sent it, she couldn't access her account again.

- If the student emphasizes the risks of sharing personal information or password details with any online entity, highlighting the importance of safeguarding such details.
- If the student points out the inaccuracy of verifying any online entity claiming to be an official organization and requesting personal information or passwords.

A bank customer service representative contacted Abdullah to verify the accuracy of his card and bank account information. After that, Abdullah received a message informing him of a withdrawal of 50,000 riyals from his account .

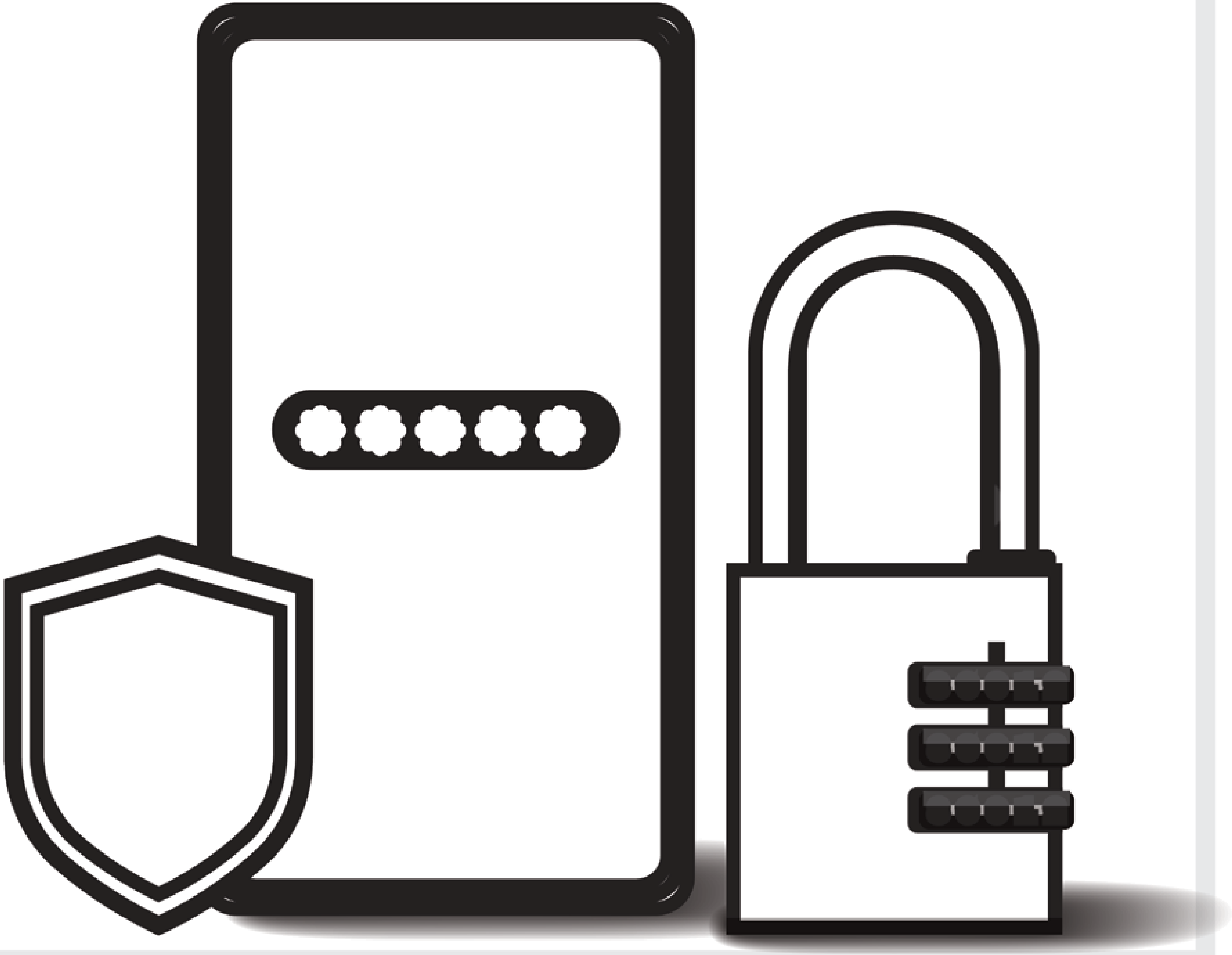
If the student emphasizes the critical nature of refraining from sharing personal or financial account information to anyone or any entity claiming to be official since banks never request customer information via phone calls.

Mona saw a sponsored ad on Facebook for a charity collecting donations for Sudanese refugees. She sent them some money, and when she tried to confirm receipt of the amount, no one responded to her.

If the student mentions that impersonating charitable organizations or humanitarian entities as a means of perpetrating online fraud, while emphasizing the importance of exclusively engaging with these organizations or associations through their official websites and validating the authenticity of donations via official receipts.

Do you know that...?

Logging into certain websites using your Facebook account details might expose you to online fraud.



The digital footprint is formed through

1. Online shopping.
2. Register to create an account on a specific website.
3. Downloading and using applications.
4. Using social media on your devices.
5. Logging into other websites using social media credentials.
6. Communicating with friends and contacts online.
7. Share information, data, and images with acquaintances.

Digital footprint protection methods

1 Verifying our information using search engines.

2 Removing personal information from websites.

3 Restricting the amount of data shared online.

4 Checking social media privacy settings.

5 Avoid unsafe websites.

6 Being cautious when using public Wi-Fi network.

7 Deleting our old online accounts.

8 Creating strong passwords.

9 Avoiding logging into websites using Facebook credentials.

10 Regularly update programs and applications.

11 Setting a password for the mobile phone.

12 Act quickly after a data breach.

Online fraud protection guidelines

1 Downloading applications from well-known app stores.

2 Regularly updating the phone.

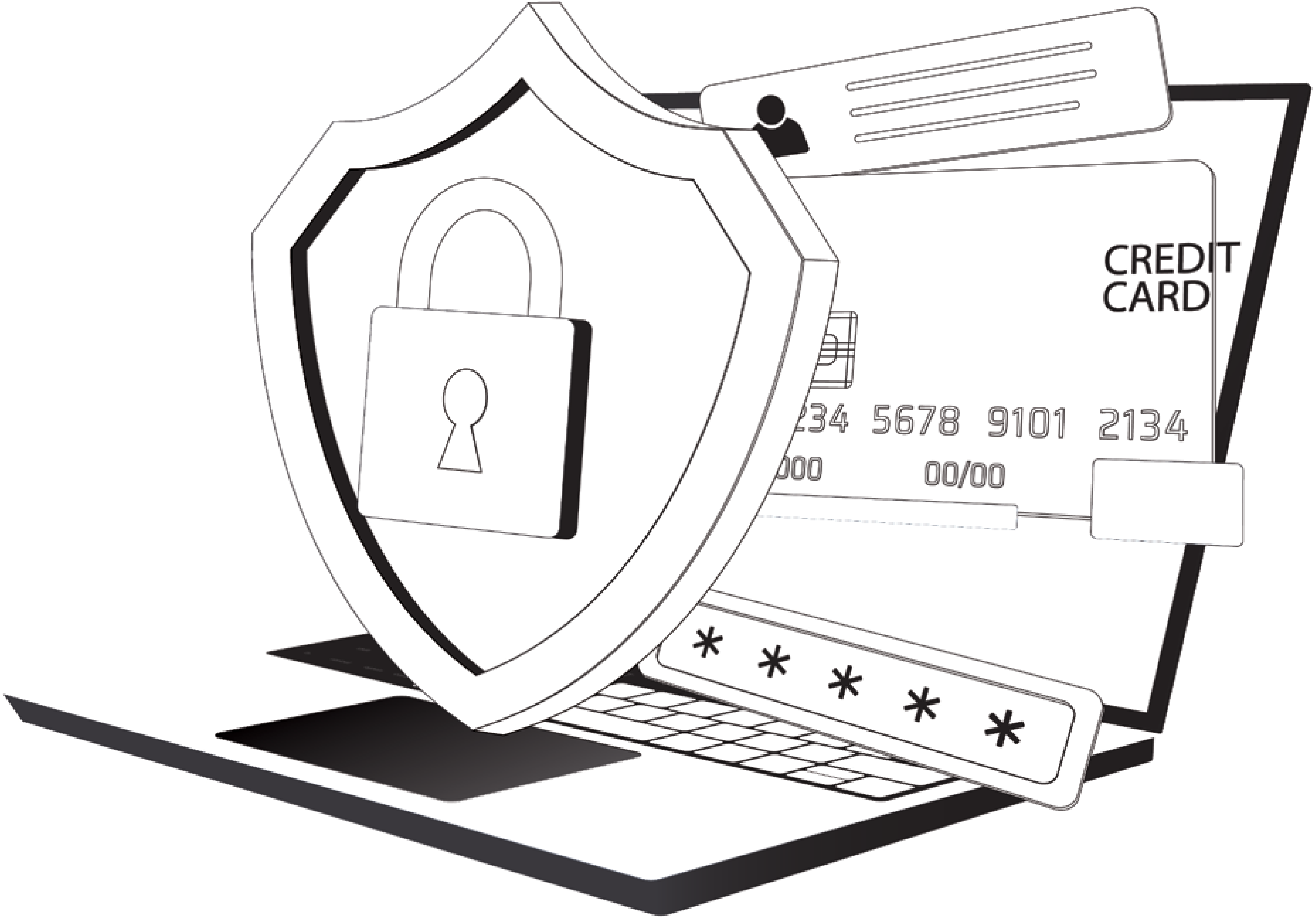
3 Avoiding unknown source links.

4 Be cautious about transactions involving third parties.

5 Employing anti-virus software.

6 Using complex passwords.

7 Refraining from shopping on unfamiliar websites.


CREDIT CARD
234 5678 9101 2134
000
00/00
* * * * *

pay attention!

Information security

Refers to a set of security measures and tools that widely protect sensitive information from misuse, unauthorized access, or destruction.

Competitions

Choose the correct answer

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

■ Posts on social media platforms.

□ Applications using geolocation.

□ Websites installing cookies without user notifying.

2. One of the most important sources of personal information is the identification links related to applications and websites.

■ True.

□ False.

3. Online fraud is usually carried out when individuals visit websites, chat rooms, online stores blogs or smart applications.

■ True.

□ False.

4. **Deception or informational cheating is associated with the concept of online fraud; it is called "information fraud".**

■ True.

□ False.

5. **Online fraud is the act of seizing others' money through deceit, using computer devices.**

■ True.

□ False.

6. **Causes of online fraud include:**

□ Misuse of internet sites.

□ The spread of fake online stores..

□ Exploitation of emotional compassion.

■ All of the above.

7. **Emails containing links to attractive financial and in-kind prizes are forms of online fraud.**

■ True.

□ False.

8. **A security vulnerability is a term used for weak spots in computer operating systems and software.**

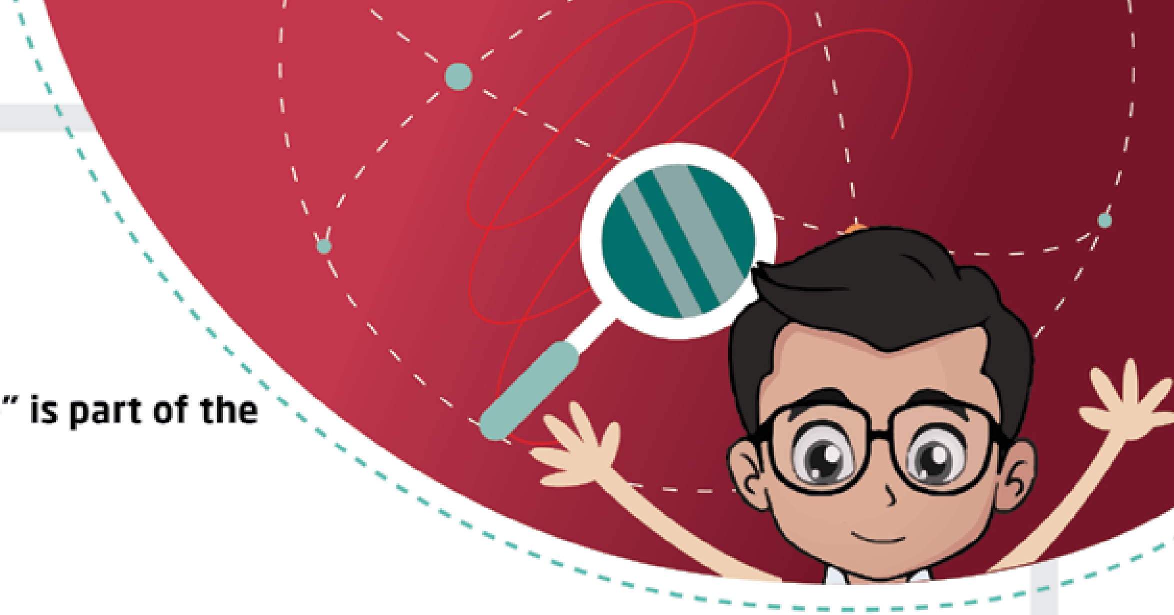
□ True.

■ False.

9. **The Zero-Day loophole does not represent a threat to cybersecurity**

□ True.

■ False.



10. The step of "Creating an Exploitation Code" is part of the Zero-Day loophole attack mechanism

☑ True.

□ False.

11. In the online world, the term "theft" is referred to as...

□ Data violation.

□ Data leakage.

☑ All of the above..

12. .... can be used to track anyone's activities online.

□ Facial recognition.

□ Handprint recognition.

☑ Digital footprint.

Find the matching item

Match the sentences from column (A) with the corresponding ones from column (B)

Column (A)			Column (B)
Causes of online fraud	○	●	Exploitation emergencies such as the COVID-19 pandemic
Fake e-mail messages	○	●	One form of online fraud
Examples of online fraud crimes	○	●	Cryptocurrency theft in recent years, such as Bitcoin
One of the security vulnerabilities that infects software	○	●	Zero-Day
A set of security measures and tools that protect sensitive information from misuse	○	●	Information security
Theft of digital information stored on computers or phones for the purpose of privacy violation	○	●	Data theft
A synonym for the word “theft” in the internet	○	●	Data breach

Place the word or phrase synonymous with the following sentences:

An attack that disables our online accounts, and in exchange for reusing them, we have to pay a sum of money. ....

Fake messages offering financial rewards and gifts arrive via email or messenger with the aim of deceiving and stealing our data. ....

Vulnerable areas that lead to infiltrating our devices, whether computer or phone, putting us at risk. ....

Tools that safeguard our sensitive information from unauthorized access, disruption, or destruction. ....

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

Online footprints used by attackers to exploit sensitive information and deceive both us and others. ....

It consists of 12 letters, symbols and numbers, and aimed at protecting us online. ....

Complete the following sentences with the correct answers:

1 ...Active... digital footprint refer to intentional sharing of user information.

2 Inactive digital footprint involve collecting user information without their knowledge.

3 Cybercriminals can exploit digital ...footprint... for purposes like identity theft.

4 Among the ways users add to their digital footprint is by downloading applications

5 Restricting the quantity of shared data is among the methods of safeguarding the digital footprint.

6 Verifying privacy settings is a way to protect **the digital footprint**

7 Avoiding clicking on **unknown source links** is among the guidelines for protection from online fraud.

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

9 In case of exposure to an online fraud, it's advisable to report it to **a trusted person like parents**

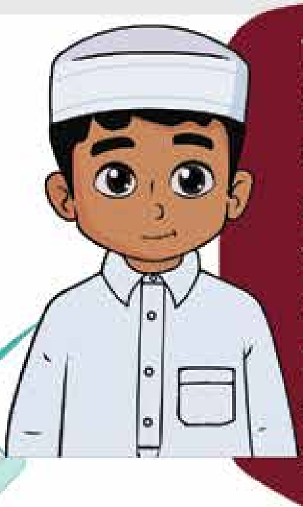
10 If your screen suddenly fills with creepy pop-ups windows, then **you should close it immediately**

pay attention!

Digital footprint

Refers to the trail of data and information left behind when using the internet. This encompasses the websites visited, the emails sent and received, and the information provided online.**The digital footprint** shapes individuals' online reputations, similar to what occurs in real life.

Graduation project

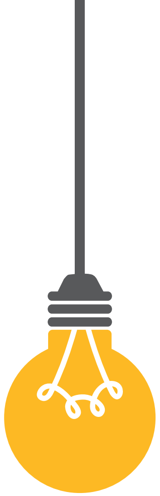


The graduation project is an assignment that you undertake on your own or in collaboration with one or two of your colleagues, under the supervision of the trainer. Through it, you are required to perform one of the following assignments:

Write a short story about a student who was experiences an attempted online fraud, and how he dealt with the situation.

The student takes on the role of a trainer and writes general guidelines to his colleagues or parents, explaining the necessary steps to protect themselves from the risks of forgery and online fraud.

References



Arabic References:

1. Protect yourself from scams and online attacks, Microsoft. Available at: https://cutt.us/YVxY1

2. The most famous electronic fraud methods that have spread in recent years, Russia Today, 2020. Available at the link: https://cutt.us/gDg5J

3. Hammadi, Khaled. Digital Footprint... The Invisible Electronic Shadow, Larbi Tebessi University, Tebessa, Algeria, July 2021, available at the link: https://cutt.us/QToSN

4. Electronic piracy: $600 million stolen in a massive digital currency scam, BBC Arabic, 2021. Available at the link: https://cutt.us/ToS7P

5. What is data theft and how to prevent it?, Kaspersky. Available at: https://cutt.us/Ve2to

6. What is Information Security?, Microsoft. Available at: https://cutt.us/CxorE

7. Younis Al-Basha, Fayza. Organized Crime under International Agreements and National Laws, Dar Al-Nahda Al-Arabi for Printing, Publishing and Distribution, 2001, p. 21.

English References:

8. 300m in cryptocurrency' accidentally lost forever due to bug, The Guardian. On site: https://cutt.us/ILdpQ

9. All 3 Billion Yahoo Accounts Were Affected by 2013 Attack, The New York times. On site: https://cutt.us/oOhv7

10. Computer and Internet Fraud, Impact Law. On site: https://cutt.us/DtS4E

11. How aligning security and the business creates cyber resilience, State of Cybersecurity Resilience 2021. On site: https://cutt.us/ZMXpW

12. How to Handle Zero-day, Nordic Defender, 2022. On site: https://cutt.us/gUQ7g

13. How to Map, Monitor and Manage Your Digital Footprint, Bitdefender. On site: https://cutt.us/G7awc

14. How to protect your digital footprint, state farm, 2023. On site: https://cutt.us/OcHUG

15. Internet Fraud, Australian Federal Police (AFP). on site: https://cutt.us/IeAYp

16. Mobile phone fraud, Action Fraud – National Fraud&Cyber Crime Reporting Centre. On site: https://cutt.us/1FoJG

17. Ransomware News, Ransomware Timeline: Top Stories December 2017, Cyber defense magazine. On site: https://cutt.us/IJBEQ

18. Report: The 2021 Identity Fraud Study, BY ALEX ROLFE, April 2021, on site: https://cutt.us/fVN5g

19. Toyota Boshoku Corporation loses $37 million in Business Email Compromise scam, CYWARE SOCIAL. On site: https://cutt.us/fFDMv

20. Varga, Gergo. 7 Types of Ecommerce Fraud & How to Detect Them, SEON. On site: https://cutt.us/TvLAe

21. VB2018 paper: Since the hacking of Sony Pictures, Minseok (Jacky) Cha, AhnLab, South Korea. On site: https://cutt.us/ZwCye

22. What is a digital footprint? And how to protect it from hackers, Kaspersky. On site: https://cutt.us/teSUS

23. What was the WannaCry ransomware attack? cloudflare. On site: https://cutt.us/8jM6q

24. What is a Zero-day Attack? - Definition and Explanation, Kaspersky. On site: https://cutt.us/FXNvU

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

26. What is email fraud? Cloudflare. On site: https://cutt.us/mg8Sf

27. Zero Day Exploit: All You Need to Know, phoenixnap, 2023. On site: https://cutt.us/Tr7jJ

CyberEco

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

CyberEco

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency