Family
Cybersecurity

Target group

Women and Family

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

Family Cybersecurity

Target group: Women and Family

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

Intellectual Property Rights

January 2025
Doha, Qatar

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

◆ Dear Participant,

In light of the rapid technological advancements and the pervasive presence of the internet in various aspects of life, cyber threats have become a challenge all segments of society encounter. This necessitates efforts to raise awareness about digital safety concepts, which serve as the shield protecting society from these threats.

As part of the «National Initiative for Digital Safety» efforts to enhance digital safety standards within the community, the National Cyber Security Agency presents this booklet with a collection of general tips and guidelines related to digital safety.

Table of Contents

Introduction

Cyber threats are not limited to businesses and companies but extend to family members of all ages. These threats range from malware and online fraud to data breaches affecting computers, smartphones, and even Internet of Things devices, leaving families vulnerable to cybercrimes. Therefore, what businesses and companies need to do to protect their interests from the effects of serious cyber threats is the same as what is required for family members. This includes relying on approved protection and anti-malware programmes, cyber awareness, and proper use of the internet.

Despite the benefits of the internet and technology in general, the cost of daily use has been accompanied by negative phenomena, such as online violence against women and children. This violence has included types of cybercrimes such as harassment, identity theft, and personal data theft, which are exploited against victims either to obtain money or to carry out services punishable by law, such as fraud against others.

Therefore, digital literacy and cyber awareness are crucial in navigating and minimising these online threats. A solid understanding of cybersecurity empowers users to safely browse the internet, utilise applications, and operate various programs. Moreover, it enhances their adaptability and resilience when confronted with diverse cyber threats, including ransomware attacks and security breaches. A sound knowledge of cyber safety equips users with effective strategies and tools to safeguard their digital devices and personal data against unauthorised access and theft.

01

Chapter One

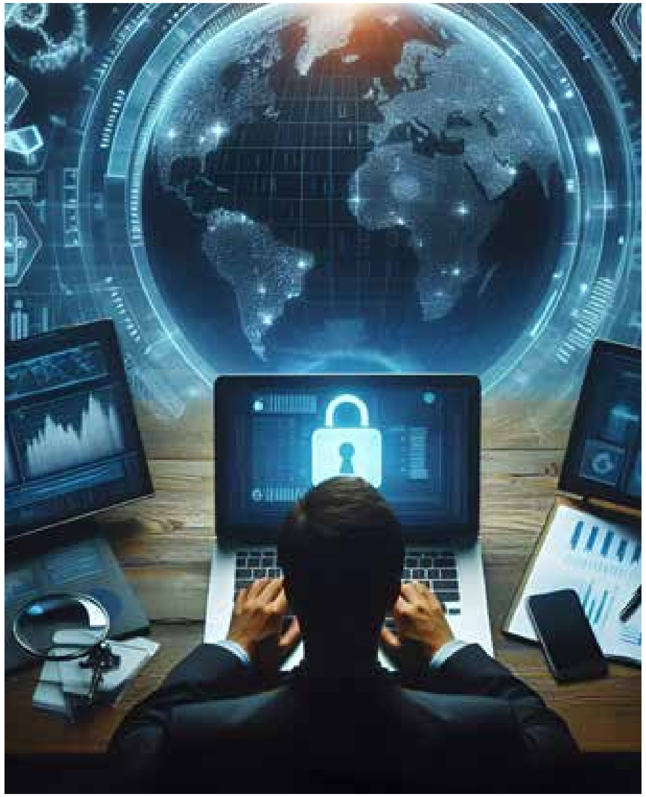
Personal Data Breaches

- First: Personal data breaches
- Second: Common methods used in data breaches:
  - Phishing
  - Malware
- Third: Data breaches and cybercrimes against women

First: Personal Data Breaches

Personal data breaches are security incidents that aim to expose sensitive information and data without authorisation. They can occur online, through Bluetooth, or via text messages. For individuals, data breaches happen because of losing computers and smartphones, infecting them with malware, or granting access to important personal data to unauthorised individuals.

In other words, data breach is any security incident in which unauthorised individuals gain access to sensitive information, including personal data such as social security numbers and bank account numbers. An example is a ransomware attack that blocks data and demands payment for its release[1].



⚠ **Beware!**

Personal data breaches aim to expose sensitive information and data without authorisation. They can occur online, through Bluetooth, or via text messages.

[1] What is a data breach? Follow link: https://www.ibm.com/topics/data-breach.

Data breaches occur through several vulnerabilities, most notably:

- ✓ **Cyber vulnerabilities:**

  These are flaws or defects in the system that criminals can discover and exploit to breach systems and steal data.

- ✓ **Knowledge gaps:**

  These are weaknesses in users' experience and insufficient knowledge of cyber safety principles. Criminals exploit this lack of knowledge to trap users and steal their personal data.

  Computers and all electronic devices, due to their connection to the internet, face increasing risks of data breaches. For example, Internet of Things (IoT) devices face some "smart home" products face flaws such as lack of encryption, which cybercriminals exploit to infiltrate family members' data[1].

  Technology isn't the only cause of data breaches; user behaviour is a key factor in such cases. If one family member behaves improperly on the internet, such as opening suspicious email attachments, this means the rest of the family is exposed to cyber threats.

Facts and Figures

- Data of 6.41 million users worldwide was leaked in the first quarter of 2023, affecting millions of individuals[2].
- More than 52% of total data breach incidents affecting global institutions in 2023 targeted customers' personal information.

[1] How Data Breaches Happen & How to Prevent Data Leaks. Follow link: https://www.kaspersky.com/resource-center/definitions/data-breach.

[2] Data breaches worldwide - Statistics & Facts. Follow link: https://www.statista.com/topics/11610/data-breaches-worldwide/#topicOverview.

Second: Common Methods Used in Data Breaches

01 Phishing

02 Malware

Phishing

Phishing is one of the most widespread cybercrimes. Attackers exploit the internet to deceive victims to steal their personal information, such as passwords and credit card numbers. This is done using various methods and tools, such as creating fake websites to attract the victim, with links sent via email or text messages to lure them. When clicking on the link, attackers can gain unauthorised access to victims' accounts and devices, installing malicious software that allows them to steal data without the user's knowledge.

In phishing, attackers rely on psychological pressure to convince victims to make quick decisions without thinking. They do this by impersonating a known person and creating a false sense of urgency, exploiting feelings of fear and anxiety to achieve their goals. Victims are often notified that they are threatened with losing money, facing legal problems, or may be denied access to important resources if they don't take immediate action, pushing the victim to respond quickly without verification.

The data targeted in phishing attacks includes:

- ✓ Usernames.
- ✓ Passwords.
- ✓ Credit card numbers.
- ✓ Bank account information.
- ✓ Any important information that, if disclosed, would harm the individual or those around.

Beware!

Data targeted in phishing attacks includes usernames, passwords, credit card numbers, bank account information, and any important information that, if disclosed, would harm the individual or those around them.

Examples of phishing:

Advanced-fee scam

This fraud is carried out via email, where the attacker presents a request to targeted victims asking for a sum of money to help them until they receive large “fictitious” sums of money. Here, victims are manipulated, exploiting their desire to obtain money through easy means.

Beware!

To avoid the risks of advanced-fee scams, check the sender’s email address before opening the message; the displayed name may be fake. Also, be wary of numbers starting with 07 as they are free to obtain. Spelling and grammatical errors are signs that lotteries and prizes in general are fraudulent.

To deal with this attack, it's advised not to comply with requests from unknown individuals that involve sending money in exchange for a service. You can search about the matter on Google to learn details of the same fraud operations that have previously been repeated to deceive others.

Example:

Lottery or financial prizes, where the scammer informs the targeted victim via email that they've won a large sum of money. If responded to, the scammer will ask for personal information and copies of official documents such as passports as proof of identity, then will request payment of certain fees for the victim to receive the prize money[1].

[1] Lottery scams. Follow link: https://www.actionfraud.police.uk/a-z-of-fraud/lottery-scams.

✓ Website forgery scam

This type of fraud is associated with other operations, such as the previously mentioned account deactivation. In this cyber-attack, fraudsters create a fake website identical to the original website of an entity, such as a bank. Once the victim visits the website, they fall prey to phishing operations. This happens through sending emails or through search engines, where the victim may visit a site believing it to be correct. The aim of this fraud is to collect user data to reuse in other crimes or to sell on the dark web.

⚠ **Beware!**

It's advised to verify the URL of websites in general in the web browser to avoid falling victim to fraud operations, ensuring the link begins with HTTPS and not HTTP.

Psychological manipulation in website forgery scams

Cybercriminals often resort to psychological and emotional manipulation of their victims to motivate them to make decisions that benefit their cyber-attacks. This is done through several methods, including:

- ✓ **Quick offers or alerts that rush the victim to take urgent action without proper thinking.**
- ✓ **Attractive promises such as gift cards or earning money, which pushes the victim not to think about the risks of implementing what's required to obtain these free gifts.**
- ✓ **False alerts about the presence of a virus that pushes the victim to intervene and implement what's requested in the messages without thinking as well.**

It's advised to verify the URL in the web browser to avoid falling victim to fraud operations, ensuring the link begins with HTTPS and not HTTP[1].

Example:

With the onset of the coronavirus (COVID-19) outbreak, fraudulent fake vaccine websites appeared. In 2020, reports emerged of false virus treatments involving collecting victims' payment information or social security numbers in exchange for experimental vaccine participation.

These websites were spotted fraudulent when they offered gifts in exchange for registering names, as well as requesting sensitive details from victims, such as bank account numbers.

[1] What Are Scam Websites and How To Avoid Scam Websites. Follow link: https://www.kaspersky.com/resource-center/preemptive-safety/scam-websites.

Information

In the first half of 2023, nearly 3 million fake websites dedicated to phishing were discovered.

Beware!

Cybercriminals create fake websites that mirror genuine ones, such as those of banks. As soon as a victim visits the site, they fall prey to phishing operations. This occurs through email messages or search engines.

Warning signs to identify fake websites:

- ✓ Appealing to emotions through urgency or fearmongering.
- ✓ Poor quality website design.
- ✓ Numerous spelling or grammatical errors in the text.
- ✓ Lack of standard web pages, such as ‘Contact Us’ or ‘About Us’.
- ✓ Mimicking original domain names; always double-check before visiting any new site by entering the URL on sites like WHOIS to verify authenticity[1].
- ✓ Requesting direct bank transfers; scammers prefer this method in their impersonation schemes, knowing it’s difficult to recover the money.
- ✓ Manually type the web address or save it in your bookmarks instead of directly clicking on sent links, which are increasingly likely to be fake.
- ✓ Verify the presence of the padlock symbol. All web browsers like Firefox and Chrome use ‘SSL security certificates’. It’s best to check for this certificate, which hinders cybercriminals from intercepting information sent to the site. To verify the presence of this certificate, look for the padlock symbol in the URL in the address bar.

⚠ **Beware!**

If you’ve responded to a fraudulent email, cut off communication with the scammer immediately.
If you’ve provided bank account details, contact your bank immediately and inform them.

[1] Ryan Toohil, How To Identify Fake Websites: 11 Warning Signs, November 2023. Follow link: https://www.aura.com/learn/how-to-identify-fake-websites.

If you‘ve visited a fraudulent website, follow these steps:

- ✓ Cut off communication with the scammer.
- ✓ Look for any pending or ongoing payments and stop them.
- ✓ Cancel the compromised credit card.
- ✓ Update passwords for bank accounts and email.
- ✓ Freeze account balances to prevent scammer access.
- ✓ Check your computer to ensure it’s free from malware or keylogging software.
- ✓ Report the fraud details to your bank, service provider (like online shopping sites), or the relevant security authority.

Beware!

Phishing aims to deceive victims into taking actions that serve cybercriminals’ malicious objectives.

Malware

Malware is a term encompassing all types of computer software that cause device damage and data breaches. It intentionally seeks to invade computers, systems, networks, tablets, and mobile devices, either to damage their systems, disable them, or steal their data. The motives behind this vary, ranging from making money to sabotaging work, political interests, or mere boasting[1] .

Malware is often spread through websites, emails, and other malicious software. It can be distributed within other files, such as image files or documents. Users themselves may unintentionally install malware after clicking on unknown links in phishing emails, downloading programs from untrusted websites, connecting the computer to an infected USB drive, or visiting a website infected with malware.

We may conclude that malware is not a virus, but a type of program designed to harm computers and their users. The most common method of detecting this software is by scanning the computer for it[2].

Removing it from the computer varies depending on the type of malware installed on the device, but the most prominent method used is antivirus programs to scan the computer and delete any detected software.

[1] Malware. Follow link: https://www.malwarebytes.com/malware.

[2] What is Malware?. Follow link: https://www.mcafee.com/en-us/antivirus/malware.html.

Types of Malware

✓ Viruses

These are harmful programs that work to disable cyber devices or destroy data and files. The danger of this software lies in its ability to easily replicate itself, leading to the infection of other devices if any files are transferred from an infected device to another. For example, if a Word file carries a malicious program, the malicious program transfers to any other device on which the Word file is opened.

✓ Ransomware

Ransomware is a type of malware that prevents users from accessing their data, exploiting their lack of experience in safe internet browsing. This software usually spreads through opening email attachments from unknown sources or downloading programs and games from untrusted sites. After installing the malware, the victim's data is encrypted so they can't access it, and decryption only occurs after paying a ransom set by the attacker. There are several types of ransomwares, and it's crucial for internet users to be fully aware of them and how they work, as awareness of this software enables them to prevent it.

Beware!
Cybercriminals often resort to psychological and emotional manipulation of their victims to motivate them to make decisions that benefit their cyber-attacks.

Computer Worms

These programs are like malicious software, but they differ mainly in that they primarily target networks. This software is characterised by its ability to replicate rapidly and spread across entire networks. It starts by infecting a specific part of the network and quickly spreads to include the rest of the network parts.

This software aims to disrupt services, such as disabling public services provided over the internet, or targeting the theft of confidential data transmitted over the network, such as customers' financial information, patient records in hospitals, educational institution data, and more[1].

Spyware

Spyware is one of the most prominent risks facing internet users and is one of the most dangerous cyber threats because users often don't realise spyware is on their device. This software remains hidden even after the device is breached and primarily aims to steal user data for later exploitation, either through blackmail or damaging their reputation. Stolen data may be used in crimes such as phishing or cyberbullying.

Spyware relies on several methods to achieve its goals, including keylogging, which tracks keystrokes made by the user to steal passwords, or accessing disk drives to steal photos and other data. Interestingly, this software doesn't destroy files but only steals them to remain unnoticed.

[1] What Is a Worm?. Follow link: https://www.cisco.com/c/en/us/products/security/what-is-a-worm.html.

Spyware differs from other cyber-attacks in several aspects, most importantly: secrecy. In the case of a ransomware attack, the user is informed after the malicious software is installed that their data has been encrypted and won't be recovered until the ransom is paid. However, in the case of spyware, the attacker doesn't notify the victim, and the attack may end without the user realising their data has been stolen[1].

✓ Trojan Horse

The "Trojan Horse" is one of the most famous and widespread malicious software, relied upon in executing many cybercrimes due to its ease of installation on the victim's device. It can be downloaded onto the device without the user's knowledge when downloading programs, games, or music files from untrusted sites. Once installed, the program begins to modify the device settings and steal user data. There are many different types of Trojan horse programs, but they all share the same working mechanism, exploiting the user's weak security to breach the device and steal information[2] .

✓ Adware

Advertisements are an essential part of the internet experience, with companies relying on gathering information about internet users to direct customised ads based on everyone's interests. However, cyber fraudsters exploit these ads to carry out their attacks by including malicious software in the ads, which can sometimes lead to browser hijacking to manipulate search engines and monitor network activities.

The negative effects of adware include:

- **Slowing down the computer:** This software consumes a large part of the processor's capacity and internet speed, slowing down the device's performance.

[1] Spyware: What It Is and How to Protect Yourself. Follow link: https://usa.kaspersky.com/resource-center/threats/spyware.

[2] Emma McGowan, Trojan viruses: Detecting and removing, May 2024. Follow link: https://us.norton.com/blog/malware/what-is-a-trojan.

- **Consuming processor resources:** Adware consumes a large amount of memory, negatively affecting the overall performance of the device[1].
- **Ad attacks:** Ads can be a source of cyber threats, where criminals can install malicious software on the victim's devices, but this only happens if the user opens ad windows, so ignoring them is an effective protection method.

Signs of Malware Infection

- ✓ Slow computer performance.
- ✓ Browser redirection, where the user is transferred to another website while browsing without their desire.
- ✓ Warnings of fictitious cyber threats accompanied by requests to purchase programs to fix the defect.
- ✓ Encountering problems during computer shutdown or startup.
- ✓ Frequent appearance of pop-up ads.
- ✓ Unexplained decrease in storage space; this is because many types of malwares contain large files that occupy storage space[2] .
- ✓ Appearance of mysterious posts on social media without user control.
- ✓ Programs running and closing without user's permission.
- ✓ Random disappearance of files from the computer.
- ✓ Unexplained increase in user activity on the internet, the reason being the malware working behind the scenes to breach the device.

[1] ADWARE. Follow link: https://www.malwarebytes.com/adware.

[2] 19 signs of malware + how to cure the symptoms, November 2022. Follow link: https://us.norton.com/blog/malware/signs-of-malware.

Ways to Protect Against Malware

- ✓ Regularly update the operating system and applications to close any vulnerabilities through which cybercriminals may launch their attack.
- ✓ Don’t click on any links that appear in pop-up windows while browsing the internet, just close the message.
- ✓ Limit the number of applications installed on devices, keeping only the important ones and uninstalling the rest.
- ✓ Use one of the device security solutions available for operating systems to ensure the device is ready to face any cyber threat.
- ✓ Don’t lend cyber devices, and check settings because if a new application appears suddenly, it may be a sign of spyware.
- ✓ Regularly back up data.
- ✓ Make sure to download only verified applications, read application reviews, and use only official app stores[1].
- ✓ Regularly check bank accounts and financial data.

[1] Protect yourself from malware. Follow link: https://support.google.com/google-ads/answer/2375413?hl=en.

How to Remove Malware from a Computer

- ✓ Disconnect from the internet.
- ✓ Next, enter safe mode.
- ✓ Start monitoring resources on the device looking for harmful applications.
- ✓ Complete the scan using antivirus software.
- ✓ Clean the web browser and clear the cache memory.
- ✓ Change all passwords.

Did you know?

71% of all data breaches have financial motives.

Third: Data Breaches and Cyber Crimes Against Women

While connected to the internet, women may be exposed to multiple types of cybercrimes primarily resulting from personal data breaches, including:

- Online defamation through disclosure of personal details or manipulated images to obtain illegal services in return.
- Cyber hacking, where cybercriminals use women's personal data to carry out illegal financial transactions and other unlawful transactions[1].
- Cyber stalking, which means intruding on women's personal accounts through social media sites, attempting to contact them for illegal purposes, or sending threatening messages through chats.

Did you know?

Women between the ages of 18 and 24 are exposed to certain types of online harassment, with 26% of them experiencing online stalking.

[1] Cyber Crime Against Women. Follow link: https://www.geeksforgeeks.org/cyber-crime-against-women/.

02

Chapter Two

Family Cybersecurity

- First: Family Cybersecurity
- Second: Women‘s Cyber Safety
- Third: The Family‘s Role in Protecting Children Online
- Fourth: What Steps Should be Taken in Case of Identity Theft?

First: Family Cybersecurity

The rapid technological development is accompanied by the evolution of cyber threats facing various segments of society, which directly impacts the family. Cybercrimes have become more professional and more damaging, given the diversity of methods cybercriminals rely on to carry out their attacks. This enhances the importance of Family Cybersecurity, positively reflecting on their cyber safety and the safety of their personal data.

Cyber safety aims to follow rules and procedures to protect computers, servers, mobile devices, systems, networks, and data from attacks carried out by malware. For networks, cyber safety aims to secure the computer network from the infiltration of cyber attackers or malware. At the application level, cyber safety means ensuring cyber devices and programs on them are free from security vulnerabilities and malware, which protects data during storage or transfer from loss or blockage in exchange for ransom payment.

Cyber safety also includes learning to ensure the correct use of the internet and its applications, programs, and websites, and training on how to deal with suspicious emails and other matters that threaten the safety of family members.

Second: Cyber Safety for Women

- ✓ It's advised not to leave the webcam connected due to applications capable of operating the camera and recording movements without the woman's knowledge. It's recommended to disable camera permission and keep its lens closed or covered when not in use[1].
- ✓ Limit sharing messages, images, or personal information, as this personal data can be used by criminals in phishing operations.
- ✓ Any device equipped with "location service" poses a risk of leaking personal data, such as location. Cautious should be exercised and this feature should be disabled.
- ✓ Regularly update all operating systems on cyber devices and use antivirus programs.
- ✓ Read the privacy policy and terms of service used online.
- ✓ Free gifts in the form of offers and deals are often full of viruses and spyware.
- ✓ Block suspicious people on social media.
- ✓ In case of exposure to any of the types of cybercrimes, women should report to the Cybercrime Combat Unit at the Ministry of Interior.

[1] Cyber safety for women. Follow link: https://us.norton.com/blog/privacy/cyber-safety-for-women.

Third: The Family's Role in Cyber Safety for Children

◆ The family's role in protecting children from the risks of artificial intelligence (AI)

With AI taking over, chatbots have become a big part of young people's lives. Kids are curious about them and use them for schoolwork and chatting.

Despite the benefits of using artificial intelligence, it may pose a danger in terms of loss of data privacy, cyber threats, and inappropriate content for adolescents and children[1]. This danger is also represented in the emergence of unknown applications that appear to be original and are used to make modifications to images. Of course, this requires accessing the photos section on cyber devices and smartphones and uploading images to start the editing process.

Parents should keep an eye on what their kids are doing online. Make sure the apps they use are safe and warn them about any apps you don't know or approve of. Being careless can put personal information like your name, address, and other stuff at risk of getting stolen.

Therefore, parents are advised to talk continuously with their children and establish close relationships with them so they can follow up on their activity on the internet in general and artificial intelligence applications in particular. Parents are also advised to keep their children away from interactive games that flood them with sales messages, making them a preferred target for advertising campaigns. In addition to the possibility of using these games to carry out fraudulent operations, hacking, and creating fake images of children through deep faking and voice cloning in exchange for money payment.

For this reason, it's recommended to discuss privacy and cyber safety with teenagers - specifically - to familiarise them with

[1] Tiffany Munzer, How Will Artificial Intelligence (AI) Affect Children?. Follow link: https://www.healthychildren.org/English/family-life/Media/Pages/how-will-artificial-intelligence-AI-affect-children.aspx

the risks of artificial intelligence and what information they need to know about it. Also, talk to them about impersonation and explain how it’s done by informing them that it’s illegal to publish images or data without their knowledge.

Facts and Figures

- In a United Nations survey, 80% of young people interact with artificial intelligence on daily basis.
- There are over 300,000 Chatbots operating on Facebook Messenger alone! But not all of them are safe.

◆ The family‘s role in protecting children from the risks of cyber games

What raises concerns about cyber games is children and adolescents spending time with strangers and communicating with them through unsupervised voice and text chats, which cybercriminals have exploited to build virtual trust with them to obtain personal data and suggest fraudulent links, aiming to download malware in the form of suggested games to start implementing their attacks.

What increases concerns is the emergence of augmented reality and virtual reality games, which require parents’ vigilance and constant monitoring of children’s behaviour to detect any changes in it.

To avoid these risks, the following is advised:

- ✓ Avoid using personal information in games and their forums such as name or location.
- ✓ Avoid downloading programs and games from untrusted sources.
- ✓ When disposing of a gaming device either by sale or abandonment, make sure to delete your personal information.
- ✓ Install and use a VPN when playing games.

The family‘s role in protecting children from financial transactions

Some parents resort to giving their children their own credit cards to conduct financial transactions themselves, or lending them their parents’ cards, but this may make them victims of fraudulent operations. Cybercriminals exploit children’s trust, then ask for card details, or transfer money to their accounts, or promise them valuable prizes. It’s preferable to educate children to avoid falling prey to various cyber-attacks, while monitoring their daily spending and setting withdrawal limits on cards, and regularly reviewing their data and balances. To prevent them from losing the card, it’s recommended to install applications on their phones instead of plastic cards.

The family‘s role in protecting children from the risks of harmful downloads

If one of the applications is not available to children, they may resort to searching for an alternative, which is often an unsafe version of the application.

Fourth: What Steps Should Be Taken in Case of Identity Theft?

Identity theft occurs when a criminal obtains someone's personal information with the aim of committing further cybercrimes, such as online fraud. This information typically includes the victim's name, address, phone number, and financial data like credit card numbers. It often results from data breaches.

Identity theft can happen because of user's mistakes or cyber vulnerabilities exploited by criminals:

- ✓ Being careless with privacy on social media platforms, such as oversharing personal information.
- ✓ Email breaches because of using the same password across multiple sites.
- ✓ Cybercriminals purchasing personal information on the dark web.
- ✓ Breaching private Wi-Fi networks or using public networks without securing sensitive data.
- ✓ Theft of smartphones or computers, exposing the owner to data breaches and subsequent identity theft.
- ✓ Some cybercriminals use card skimming devices on ATMs to steal and store data from the card's magnetic strip.

If you suspect your identity has been stolen, follow these steps:

- ✓ Be aware that identity theft risks are higher with common online services like shopping websites and banking. Look out for signs such as unauthorised purchases or changes to your contact details with official bodies like banks[1].
- ✓ Upon discovering identity theft, immediately notify your credit card issuers to close the accounts and change all your passwords.
- ✓ Place a fraud alert on your credit report. This hinders attempts by the fraudster to open new accounts using the stolen identity without the financial institution contacting you first for verification.
- ✓ Review your credit reports as soon as the alert is activated. It's advisable to check each of your credit reports again over the following year to ensure there are no ongoing signs of identity theft.
- ✓ Report the incident to your local cybercrime unit at the police department.
- ✓ Contact your service providers and phone companies to inform them of the identity theft. This can thwart the fraudster's attempts to exploit your identity or open accounts with it.
- ✓ Use antivirus software to handle common and complex threats such as viruses, malware, ransomware, and spyware applications.

[1] Identity theft and identity fraud: What to do if your identity is stolen. Follow link: https://www.kaspersky.com/resource-center/threats/what-to-do-if-your-identity-is-stolen-a-step-by-step-guide.

Exercises

The following questions are based on the material covered in this booklet. Answers can be found at the end of the booklet.

Exercise One

- **Choose the correct answer**

1. For cybersecurity, it's advised not to use .... as they help cybercriminals infiltrate connected devices through man-in-the-middle attacks.

1 Contact details

2 Public Wi-Fi networks

3 Passwords

2. Women face online harassment, including ....

1 Rumours

2 Cyberbullying

3 Cyberstalking

4 All the above

3. One sign of malware infection is ....

1 Browser redirects

2 Random appearance of files

3 Decreased user activity on the internet

4. Cybercriminals collect sets of stolen (usernames and passwords) to test on websites to access user accounts, known as ....

1 Brute force attacks

2 Credential stuffing

3 Trojan horses

5. A type of brute force attack where the attacker needs prior knowledge of the victim's name to start trying possible passwords is ....

1 Reverse brute force attack

2 Hybrid brute force attack

3 Dictionary attack

6. One of the warning signs for identifying fake websites is ....

1 Avoiding emotional appeals

2 Moderate spelling and grammatical errors

3 Mimicking original domain names

7. All web browsers like Firefox and Chrome contain what's called ....

1 A warranty certificate

2 An SSL security certificate

3 A reliability certificate

8. If you visit a fraudulent website, you should ....

1 Continue communicating with the scammer to understand their goals

2 Only update passwords for bank accounts

3 Look for any pending or ongoing payments and stop them

Exercise Two

Write “True” next to the correct statement and “False” next to the incorrect one. If false, correct the statement.

1. Computer worms lack the ability to copy themselves from one device to another and need the user to start the attack.

2. Spyware is installed on the computer with the user’s knowledge.

3. Trojan horse malware disguises itself as harmless applications to trick users into downloading and using them on their computer.

4. One sign of malware infection is decreased storage space on the device.

5. Brute force attacks are common methods used in data breaches.

Exercise Three

Complete the following statements

1. Psychological manipulation in website forgery scams is done through several methods: .... , ... , ...

2. Warning signs indicating fake websites include .... , ... , ...

3. To prevent account deactivation scams, it's advised to .... , ... , ...

4. Data targeted in phishing attacks includes .... , ... , ...

5. Data breaches occur due to weaknesses in .... , ... , ...

Answer Key of Exercises

Question

Exercise One: Choose the correct answer

Answer

1. Public Wi-Fi networks
2. All the above
3. Browser redirects
4. Credential stuffing
5. Hybrid brute force attack
6. Mimicking original domain names
7. An SSL security certificate
8. Look for any pending or ongoing payments and stop them

Question

Exercise Two: Write "True" next to the correct statement and "False" next to the incorrect one. If false, correct the statement.

Answer

1. **False.**

   A computer worm is self-replicating malware that duplicates itself to spread to uninfected computers, exploiting security weaknesses in a program or operating system, and don't need the user to start the attack.

2. **False.**

   It's installed on the computer without the user's knowledge to collect personal information or monitor internet browsing habits and transmit them to the attacker, enabling them to monitor all forms of communication on the targeted device.

3. **True.**

4. **True.**

5. **True.**

Question

Exercise Three: Complete the following statements

Answer

1 Psychological manipulation in website forgery scams is done through several methods:

- Quick offers or alerts that rush the victim to take urgent action without good thinking.
- Attractive promises such as gift cards or earning money.
- False alerts about the presence of a virus that pushes the victim to intervene and implement what's requested in the messages without thinking.

2 Warning signs indicating fake websites include Appealing to emotions through urgency or fear-mongering - Poor quality website design - Numerous spelling and grammatical errors.

3 To prevent account deactivation scams, it's advised to Not to open attachments or links in suspicious emails - Perform all downloads from official stores - Install and regularly update antivirus software.

4 Data targeted in phishing attacks includes Passwords - Credit card numbers - Bank account information.

5 Data breaches occur due to weaknesses in Technology - User behaviour.

References

1. What is a data breach?. Follow link: https://www.ibm.com/topics/data-breach
2. How Data Breaches Happen & How to Prevent Data Leaks. Follow link: https://www.kaspersky.com/resource-center/definitions/data-breach
3. Data breaches worldwide - Statistics & Facts. Follow link: https://www.statista.com/topics/11610/data-breaches-worldwide/#topicOverview.
4. Lottery scams. Follow link: https://www.actionfraud.police.uk/a-z-of-fraud/lottery-scams
5. What Are Scam Websites and How To Avoid Scam Websites. Follow link: https://www.kaspersky.com/resource-center/preemptive-safety/scam-websites
6. Ryan Toohil, How To Identify Fake Websites: 11 Warning Signs, November 2023. Follow link: https://www.aura.com/learn/how-to-identify-fake-websites
7. Malware. Follow link: https://www.malwarebytes.com/malware
8. What is Malware? Follow link: https://www.mcafee.com/en-us/antivirus/malware.html

9. What Is a Worm? Follow link: https://www.cisco.com/c/en/us/products/security/what-is-a-worm.html
10. Spyware: What It Is and How to Protect Yourself. Follow link: https://usa.kaspersky.com/resource-center/threats/spyware
11. Emma McGowan, Trojan viruses: Detecting and removing, May 2024. Follow link: https://us.norton.com/blog/malware/what-is-a-trojan
12. ADWARE. Follow link: https://www.malwarebytes.com/adware
13. 19 signs of malware + how to cure the symptoms, November 2022. Follow link: https://us.norton.com/blog/malware/signs-of-malware
14. Protect yourself from malware. Follow link: https://support.google.com/google-ads/answer/2375413?hl=en
15. Cyber Crime Against Women. Follow link: https://www.geeksforgeeks.org/cyber-crime-against-women/
16. Cyber safety for women. Follow link: https://us.norton.com/blog/privacy/cyber-safety-for-women
17. Tiffany Munzer, How Will Artificial Intelligence (AI) Affect Children?. Follow link: https://www.healthychildren.org/English/family-life/Media/Pages/how-will-artificial-intelligence-AI-affect-children.aspx
18. Identity theft and identity fraud: What to do if your identity is stolen. Follow link: https://www.kaspersky.com/resource-center/threats/what-to-do-if-your-identity-is-stolen-a-step-by-step-guide

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative