Unlicensed Software Downloads & Their Risks

Target Group
Expatriate Workers

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

Unlicensed Software Downloads and Their Risks

Target Group: Expatriate Workers

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

Considering 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	Page

Introduction

The “Baby” computer is considered the first digital computer designed with internal programming capability. It was built in Manchester in 1948. The computer uses a set of instructions to perform specific tasks to achieve expected results. It includes memory where programs are stored, enabling the computer to execute various tasks sequentially. The concept of internally stored programs was introduced in the late 1940s by Hungarian-born mathematician John von Neumann [1].

A program is prepared by first understanding the nature of the task, followed by creating the corresponding code. A computer program is developed using one of the programming languages. Computers are equipped with various programs, primarily designed to assist users in running tasks or improving system performance. These programs are as essential as the hardware components of the computer system. Consequently, downloading any software from an unreliable source may cause the entire system to malfunction or crash, thus failing to complete the assigned tasks.

With the increasing availability of various channels to obtain computer software, often free of charge, some users may resort to downloading it from unknown or unauthorised sources. Therefore, it is always advised to download computer software from official sources, ensuring it is licensed to avoid security vulnerabilities that could lead to attacks on the computer by malicious software, such as viruses, spyware and other threats.

1. Computer program. Follow link: https://www.britannica.com/technology/computer-program

01

Chapter One

Software and Piracy

- First: **Computer programs and Their Types**
- Second: **Software Piracy and Its Types**
- Third: **Risks of Downloading Unlicensed Software**

Software and Piracy

Computer programs are among the most important tools in our daily lives, whether for personal or professional use, as they improve productivity and save time.

With the increasing spread of technology and the reliance of individuals and institutions on software, the issue of software piracy has emerged, which includes illegal copying or using programs without purchasing a valid license.

Undoubtedly, software piracy poses a threat to global economies and negatively affects software developers by reducing revenues needed for innovation and development. It also heightens the risks of users falling victim to cyberattacks due to downloading unreliable or modified software.

First: Computer Programs and Their Types

A computer program is defined as a system consisting of one or more coded instructions designed to perform a specific task on a computer. When these instructions carry out a function, such as starting the device, they are referred to as "software."

These instructions can also be used to perform various tasks, such as storing files. Additionally, a set of coded program instructions can be developed using a programming language, which converts commands into a form of machine-readable code that the computer can interpret and execute.

Did you know?

As a result of the threat posed by unlicensed programs, Microsoft has issued more than 50 security bulletins related to Windows since 2003, due to the danger of attackers infiltrating users' computers through weaknesses in the operating system [(2)].

2. How Unlicensed Software Can Compromise Your Data. Follow link: https://www.bluechipit.com.au/how-unlicensed-software-can-compromise-your-data/

Major Types of Application Software:

Internet Browser

A program used to access different web pages, such as search sites or websites. The browser does not display search results but relies on search engines (such as Google) to retrieve required information. By entering a website address or keywords in the address or search bar, the user is directed to relevant results through the search engine [3].

3. What is a web browser?. Follow link: https://www.mozilla.org/en-US/firefox/browsers/what-is-a-browser/

The web browser is designed to display text, images, videos and other content from across the globe. Hyperlinks within web pages allow users to navigate between different pages. Each web page or file contains a URL (Uniform Resource Locator), which helps the browser locate and display the desired content to the user.

Did you know?

Cookies store certain user data, such as preferences or login information, on their device to speed up their experience on future visits to the website. Some cookies may store detailed information about user interests to display targeted advertisements. Third-party cookies collect data about the user across multiple sites for marketing purposes. Some browsers allow blocking such cookies [4].

Did you know?

While most browsers offer private browsing modes (such as Incognito Mode), this feature does not anonymize the user's identity or browsing data from Internet Service Providers (ISPs) or governments. Instead, it prevents the browser from saving the browsing history and passwords on the device, making it beneficial for use on public computers.

4. What are Cookies?. Follow link: https://www.kaspersky.com/resource-center/definitions/cookies

Word Processor

A word processor is a software application designed for entering, editing and formatting text. It allows users to modify the text's appearance, such as adjusting font sizes or organising paragraphs, and enables them to incorporate visual elements like tables or charts. Additionally, it provides the ability to manage editing permissions when sharing the document with others.

Most word processing programs include tools for spell checking and grammar checking, and some programs provide a thesaurus to help users improve writing quality.

Teleconferencing Software

These programs allow audio and video communication between remote users and are widely used in professional meetings, particularly due to the increasing trend of remote work. They enable participants to join video or audio meetings, and the quality and number of allowed participants vary based on the program used.

These programs have become essential to reduce financial costs associated with traditional in-person meetings and office rentals.

5. What Is Video Conferencing Software?. Follow link: https://www.bigcommerce.com/glossary/video-conferencing-software/

Digital Spreadsheets

Digital spreadsheets, such as Microsoft Excel, are powerful tools for storing and organising data in tabular format using rows and columns. They enable users to perform advanced calculations and sort data in a way that improves readability and interpretation [6].

These programs support importing of external data, modifying various templates according to user needs and sharing documents with colleagues.

Project Management Tools

These applications are used to organise and plan tasks in collaborative work environments. They provide features for assigning tasks among team members, tracking progress and setting project deadlines [7]. These tools assist managers in monitoring work progress and efficiently distributing workloads among employees, which in turn improves productivity and reduces downtime.

6. Katie Terrell Hanna, spreadsheet. Follow link: https://www.techtarget.com/whatis/definition/spreadsheet
7 . Deepak Palasamudram, What is Project Management?, Dec 2022. Follow link: https://2u.pw/RYVwfkV4

Second: Software Piracy and Its Types

Software piracy refers to the illegal and unethical use of licensed computer programs, including copying, stealing, distributing, modifying, or transferring them through unlawful means. This definition encompasses any individual's participation in such actions, whether intentional or not, as simply using software in unauthorised ways or copying and distributing licensed programs without the owner's authorisation constitutes piracy [8].

Warning!

The illegal process of software piracy includes copying programs, stealing them, or sharing them with others, as well as using such software unlawfully without the owner's authorisation.

Did you know?

In June 2018, research revealed that 37% of software downloaded on desktop or laptop computers was unauthorised.

8. What is Software Piracy?. Follow link: https://www.javatpoint.com/what-is-software-piracy

Types of Software Piracy

Softlifting or End-User Piracy

Softlifting piracy occurs when purchasing a single version of the program and subsequently installing it onto multiple devices, thus violating the licensing agreement. This action is usually motivated by a desire to save money or to make a profit, but is considered illegal nonetheless.

License Overuse

This type of piracy occurs when several users on the same network use an original copy of the program simultaneously, or when many users access the program despite restrictions limiting its use to a specific number.

Counterfeiting

Software that is illegally copied and distributed is referred to as counterfeit or pirated. These copies are often sold at a significantly lower price than the original program's original cost [9].

9. Software Piracy Facts. Follow link: https://hypertecsp.com/knowledge-base/software-piracy-facts/

Online Piracy

This term refers to cases where software is obtained illegally and then distributed online. Peer-to-peer (P2P) file-sharing networks often allow users to store and share copyrighted original software without authorisation.

Hard Disk Loading

This type of piracy involves an individual purchasing a legitimate software, installing it and then copying the software onto a computer's hard disk and selling that computer.

Warning!

Copying legally purchased software, installing it onto a computer's hard disk, and then selling the device is considered a form of software piracy.

Information

In 2012, a study revealed that 97% of all business-related materials are stored digitally, with the value of this data estimated at $1.7 trillion annually. This causes significant potential losses if such data falls into the hands of cybercriminals.

Motivations for Downloading Unlicensed Software

Financial Cost:

Unlicensed programs are usually free or cheaper than official versions. Therefore, some users and even companies seek to download pirated softwares to cut costs.

Availability:

Some programs are not available in application stores, and thus some users search for them from other unreliable sources.

Additional Functions:

Unlicensed programs contain features and additional functions not found in original programs, making them more attractive to users.

Ease of Download:

Some users resort to downloading unlicensed programs because they are easy to download, unlike original programs which require verification before downloading.

Did you know?

According to the 2018 Global Software Survey, 37% of software programs installed on personal computers were unlicensed.

Warning!

Illegally copying and distributing computer software is a form of software piracy, referred to as counterfeiting or imitation. These unauthorised copies are often sold at a price lower than the original software's actual cost.

Third: Risks of Downloading Unlicensed Software

Cyber threats are growing significantly, and with the increasing reliance on electronics to perform many daily and professional tasks, these devices are constantly exposed to viruses and malware. These threats can result in sensitive data breaches, financial losses and even identity theft. The consequences vary for individuals and businesses, as followed:

At the Individual Level

Malware Infection

Installing unlicensed software on computers increases the chances of encountering malware. For example, in 2017, a widespread attack of malware known as WannaCry infected more than 300,000 computers worldwide through harmful downloads [10].

Unlicensed (pirated) programs also promote the spread of Trojan horses and botnets. Trojans appear as legitimate programs but grant attackers remote control over the victim's system. On the other hand, botnets allow attackers to control infected devices and perform illegal activities without the user's awareness [11].

Furthermore, unlicensed programs are associated with the spread of ransomware, causing user files to be disabled and encrypted in exchange for money. If payment is not made, the cyber attacker either destroys the encryption key or publishes the stolen files on the internet.

10. Investigation: Wanna Cry cyber attack and the NH 27 October 2017. Follow link: https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs
11. What is Pirated Software?. Follow link: https://cyberpedia.reasonlabs.com/EN/pirated%20software.html

Warning!

Bots allow attackers to control infected devices to perform illegal functions without the user's knowledge.

This is primary caused by installing unlicensed programs.

Loss of Personal Data

Downloading from untrusted sources puts sensitive data at risk. Intruders can employ various methods, such as phishing and keylogging, to steal users' personal and financial information, leading to identity theft, financial fraud, and other serious consequences. In 2018, the personal information of millions of Facebook users was compromised due to a data breach caused by a third-party application.

Spyware Risks

Unlicensed software creates vulnerabilities that cyber attackers can exploit to infiltrate user or company networks, resulting in data breaches and privacy violations.

Spyware, a type of malware, covertly monitors computer activities to steal personal information such as passwords and credit card details. Downloading unlicensed software increases the risk of exposure to spyware.

System Instability

The absence of legal notifications or support from the software's manufacturer increases the likelihood of unlicensed software malfunctioning. This is due to the lack of patches and updates that are provided for legitimate programs [12].

As a result, such programs can cause system instability, frequent crashes and data loss, leading to prolonged repair times and reduced productivity, especially when the software is used in a professional setting.

Warning!

Not receiving notifications or support from the software's manufacturer due to illegal installation greatly increases the risk of unlicensed software malfunctioning, as it lacks the updates and patches provided to legitimate versions.

Legal Consequences

Software piracy is a crime punishable by law under copyright regulations designed to protect the interests of developers. Violators may face hefty fines or criminal charges.

12. Devin Partida, Why You Shouldn't Use Pirated Software (But Why People Still Do), 2020. Follow link: https://www.computer.org/publications/tech-news/trends/why-you-shouldnt-use-pirated-software

Compatibility Issues

Unlicensed software is not subject to the necessary testing to ensure compatibility with computer hardware and software, leading to what is known as compatibility issues, which can cause the computer to malfunction or fail to perform tasks properly [13].

Financial Losses

Although unlicensed software may be free, it still imposes hidden costs on users. These costs often include intrusive pop-ups or unwanted ads, requests for payment to access full features, or even enrolling users in paid subscriptions without their consent.

Compromised Security Updates

Unlicensed software may interfere with computer security updates, leaving the system vulnerable to new cyber threats. This is particularly dangerous as cybercriminals continually develop new methods to exploit known software vulnerabilities.

13. Don't Risk It: The Top 10 Dangers of Downloading Unverified Software, March 2023. Follow link: https://www.lockwell.co/blog/don-t-risk-it-the-top-10-dangers-of-downloading-unverified-software

Warning!

Unlicensed software does not undergo the necessary testing to ensure compatibility with computer hardware and software, leading to compatibility issues that can cause system crashes or prevent the computer from functioning properly.

Did you know?

A malware attack costs an average of $2.4 million per company and takes about 50 days to resolve.

At the Company Level

Data Privacy Risks

When employees purchase and use third-party software without informing the IT department, they expose sensitive data to potential risks. This decentralized control over software prevents the IT team from implementing necessary security measures, as unauthorised software hinders their ability to mitigate risks effectively.

Compliance Risks

Software is protected by intellectual property rights, and unauthorised use can lead to fines, legal penalties and the loss of sensitive data due to serious security vulnerabilities in such software, which does not receive the same patches as licensed software.

02

Chapter Two

Risks of Unlicensed Software

- First: Most Common Viruses Associated with Unlicensed Software
- Second: Warning Signs of Unlicensed Software
- Third: Protection from Unlicensed Software

Risks of Unlicensed Software

Unlicensed software is a major source of security and economic risks in the digital age. While some individuals use this software to avoid licensing fees, they often overlook the hidden threats. Unlicensed software is frequently modified or compromised, making it vulnerable to malware and viruses that can lead to system breaches and the theft of sensitive data. In addition to these security risks, users may face legal issues and financial penalties for violating intellectual property rights. Using licensed software ensures optimal performance, security and compliance with the legal regulations.

First: Common Viruses Associated with Unlicensed Software

Viruses linked to unlicensed software are among the most dangerous security threats in today's technological world. These viruses exploit vulnerabilities that arise when users download unlicensed or pirated software from untrustworthy sources. Such software often contains malicious code embedded by cybercriminals, who take advantage of individuals seeking to acquire software for free or at a reduced price.

The following are some of the most common viruses associated with unlicensed software:

Conficker Worm

Conficker worm is a computer worm that targets the Microsoft Windows operating system. It was first discovered in November 2008, and spreads by exploiting security vulnerabilities in Windows software. The worm executes dictionary attacks to crack passwords. The virus was particularly difficult to combat due to its use of various advanced malicious software techniques [14].

The computer worm is notable for its rapid spread, its ability to disable security features, stop automatic backup settings, delete restore points, and open communication channels to receive commands from a remote computer. Once it infects the first device, it spreads across the network by copying itself into shared folders.

One of the primary reasons for the spread of this type of malware is the use of unlicensed or counterfeit software. The Conficker worm, which spread globally between 2008 and 2009, serves as a notable example. At the time, cybersecurity experts emphasized the risks of downloading unlicensed software, which is one of the most common ways to such threats.

Warning!

More than 500,000 new types of malwares are produced daily [15].

14. Lital Asher-Dotan, What is the Conficker worm. Follow link: https://www.cybereason.com/blog/what-is-the-conficker-worm
15. How Unlicensed Software Can Compromise Your Data.
Follow link: https://www.bluechipit.com.au/how-unlicensed-software-can-compromise-your-data/

Did you know?

A survey conducted by the National University of Singapore on pre-assembled computer purchases in 11 countries worldwide, where unlicensed software is installed, revealed that:

- 61% of devices were infected with malware.
- 24% of malware bundled with unlicensed software downloads caused the deactivation of antivirus programs on computers.
- About 31% of incomplete pirated software installations redirected traffic to sites, exposing users to malware and unwanted advertisements [16].

16. Raja Viswanathan, Remote work, pirated software, and local admin rights: A deadly cocktail.

Second: Warning Signs of Unlicensed Software

- The appearance of a system scan prompt on the computer screen requires caution, especially with pop-up ads for software. If an ad, often disguised as a “warning or alert,” appears and prompts a system scan for malware, it is important not to click on it.

  Many fake pop-ups install keylogging software to steal users’ login credentials. Therefore, it is recommended to purchase antivirus and malware protection software from reputable websites [17].

- Warnings about the computer being infected with viruses may be misleading. These alerts often suggest installing a program to clean the system, but doing so could result in additional malware infections.

- Requesting personal information: Fraudulent activities often occur through infected emails, providing a means to install malware on the system. In this case, unlicensed software generates alerts resembling those of antivirus programs. When the user clicks on these alerts, they are requested to provide personal information, such as credit card numbers and other sensitive details.

17. Do You Know How To Spot Fake Software And Updates? Learn The 7 Red Flags!. Follow link: https://www.alvareztg.com/do-you-know-how-to-spot-fake-software-and-updates-learn-the-7-red-flags/

- Pop-up window requesting additional updates: While browsing the web, a pop-up window may appear claiming that a program needs updating, or there is difficulty displaying the page. In fact, these windows are deceptive; they contain malware that gets downloaded to the device once interacted with.
- Receiving warnings from a program you haven›t downloaded: Some users fail to regularly check the installed programs on their devices, making them vulnerable to deceptive warning messages, which they may click on before verifying if the program is installed on the device. This is common on personal computers.
- Receiving warnings in the form of pop-up messages indicating that the browser is outdated: This is a key indicator of unlicensed software, which may cause the unsuspecting user to enter fake websites that steal their personal data.
- The lack of updates or customer support for unlicensed software, unlike legitimate software that offers automatic updates and customer assistance.
- Deceptive offers: It is important to be extremely cautious about offers that provide costly software for free, as these are often unlicensed programs that can damage devices [18].

18. Clare Stouffer, Are you accidentally pirating software?, January 2024. Follow link: https://us.norton.com/blog/malware/accidentally-pirating-software

Third: Protection from Unlicensed Software

- It is essential to use reliable sources when downloading software, such as official app stores like Google Play, as they have security measures that reduce the risks of malware and cybersecurity threats.
- Be cautious about clicking on pop-up ads or unknown links, as they may direct you to unreliable advertisements.
- It is important to use reputable antivirus programs and ensure they are regularly updated to detect and remove malware from the computer.
- Be cautious of free downloads as they tend to attract individuals seeking to avoid expenses. It is essential to look for reputable sources and read reviews before initiating any download.
- Use a Virtual Private Network (VPN) to provide an additional layer of security by encrypting the internet connection and hiding the user's IP address, making it more challenging for cybercriminals to access users' devices.
- Compliance with cybersecurity best practices, including keeping software and systems updated, securing and regularly patching them against vulnerabilities and training users to identify suspicious activities, contributes to enhancing protection alongside using antivirus programs.

How to Ensure the Safety of the Software Download Process?

Verify the Legitimacy of the Website

It is crucial to check the reputation of the website first when downloading a program or application from the internet. For instance, downloading software from the well-known company Microsoft indicates that the site is safe; however, this may not apply to all websites. It is always preferable to download software created by Microsoft from the official website.

In general, to verify the legitimacy of a website, there are two methods:

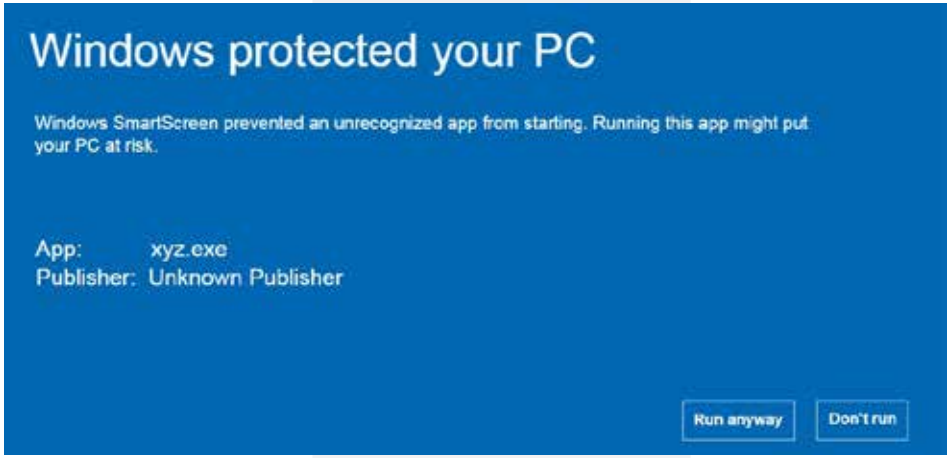
- **Verify the SSL/TLS Certificate Details:** : If you see a security lock symbol or "HTTPS" in the address bar before the website's URL, this indicates that it is secure. This should be confirmed alongside the identity of the entity owning the site, such as Microsoft, rather than an unknown entity [19].

Illustrative Image of Security Indicators on a Legitimate Website

19. How to check if a file is safe to download. Follow Link: https://www.microsoft.com/en-us/edge/learning-center/how-to-check-if-a-file-is-safe-to-download?form=MA13I2

- **Verify the pop-up notifications from Windows Defender SmartScreen,**, as it is an important security feature that automatically checks for dangerous downloads. It is advisable to enable this feature on both personal and mobile devices running Windows. For example, when attempting to download software from an unknown source using Microsoft Edge or any other browser, a warning message will appear indicating the potential risk of device damage or data theft.

  However, if a software developer has signed their code with an Extended Validation Code Signing Certificate, Microsoft will automatically trust it, preventing warning messages from appearing [20].



Illustrative Image of Warning Messages in the Windows System

20. Microsoft Defender SmartScreen. FOLLOW LINK: https://learn.microsoft.com/en-us/windows/security/operating-system-security/virus-and-threat-protection/microsoft-defender-smartscreen/

Verifying the File Size and Extension

If the file size of the intend download from the internet is significantly smaller or larger than expected, it may not be safe. Cybercriminals often create files that closely mimic legitimate software to deceive users into downloading them.

It is also crucial to verify the extension of all files to ensure their legitimacy. For instance, a Word document should not be classified as an executable file (exe) [21].

Checking User Reviews of the Software

Reviewing user experiences related to the software before downloading can help avoid many issues from the beginning. Therefore, before downloading any mobile application from the Apple App Store or Google Play Store, it is essential to check the reviews. If the ratings are poor, it is advisable to avoid downloading the application.

Using Antivirus Software to Scan Downloads for Malware

Antivirus softwares assist in detecting and removing viruses and various types of malwares. Therefore, if a user is about to download an executable file, such as ".exe" they should be cautious, as any malware within the file could infect the computer system and compromise its data security.

21 . How Can I Tell If a Download Is Safe?. FOLLOW LINK: https://codesigningstore.com/how-to-tell-a-download-is-safe

Caution When Downloading and Opening Email Attachments

Downloading an infected or malicious attachment sent via email from unknown sources can compromise the entire system and expose data to significant risks. Cybercriminals use specific types of files, such as executable (.exe) files, compressed files, and Office documents, to spread malware and execute their cyberattacks. To avoid this, users should refrain from downloading attachments from unknown contacts.

Information

According to data from the 2018 Data Breach Investigations Report (DBIR) published by Verizon, over 90% of malware spreads through email messages.

Exercises in this part are based on the presented material. An answer key is provided at the end of the booklet.

Exercise One

• Choose the correct answer

1. Computer programs can be used to perform various functions, including .....

1. Searching for information on the internet
2. Classifying and storing data on the computer
3. Protecting the computer from malicious software such as viruses
4. All of the above

2. Cookies perform the following function .....

1. Selling user information to external parties
2. Activating incognito mode on main browsers
3. Storing user information on their computer for reuse when visiting websites

3. Types of software piracy include .....

1. Trojan horses
2. Hard disk loading
3. Viruses

4. ..... refers to the unauthorized copying and distribution of software for imitation. These copies are often sold at a price lower than the real price of the original program.

1. Internet piracy
2. Hard disk loading
3. Counterfeiting or imitation

5. Reasons for downloading unlicensed programs include .....

1. Lower financial cost comparable to original programs
2. Difficulty in downloading before verification
3. Inclusion of additional features and functions

Exercise Two

Write "True" before correct statements and "False" before incorrect ones, and correct the false statements:

1. Third-party cookies are not related to websites visited by users, but rather track users across sites to collect information about them and sell it to external parties.

2. Some cookies retain more precise information, such as user interests, to direct them to compatible content.

3. It is a common misconception that "incognito mode" conceals the user's identity and browsing history from Internet Service Providers (ISPs), governments, and advertisers.

4. The Word processor assists when sharing a document with others by limiting access to editing the document's content.

5. Digital spreadsheets complicate organising data into clear columns, rows and sections, making it more difficult for users to read and understand the information.

6. Digital spreadsheets enable the scheduling of work tasks and the organisation of current or planned activities for everyone in the workplace on a single digital board.

7. Software piracy refers to anyone who participates in the unauthorized use, copying, or distribution of licensed software, intentionally or not.

8. Receiving warnings about computer virus infections is one indicator of pirated programs.

9. Using a Virtual Private Network (VPN) helps hide the IP address, making it difficult for cybercriminals to access users' devices.

10. Pirated programs refers to programs that are authorised and legally copied for distribution or sale without owner authorisation.

11. Using pirated programs leads to legal consequences, such as imprisonment. However, financial fines are not required in all cases.

12. Reading programs installation requirements before downloading is not required as long as it is done through approved application stores.

Exercise Three

Fill in the appropriate term

1. It is incorrect that ..... hides user identity and browsing history from Internet service providers governments, and advertisers..... programme helps in setting limits to others' access to editing document content.
2. ..... program helps set restrictions on others' access to editing document content.
3. ..... allows colleagues to communicate remotely instead of in-person meetings.
4. ..... are applications that can be used in scheduling work duties, facilitating easy collaboration with the work team, regardless of distance.
5. ..... refers to obtaining or spreading illegal programs via the internet.

Answer Key

Question

Exercise One: Choose the correct answer

Answer

1. All of the above
2. Storing user information on their computer for reuse when visiting websites
3. Hard disk loading
4. Counterfeiting or imitation
5. Inclusion of additional features and functions

Question

Exercise Two: Write "True" before correct statements and "False" before incorrect ones, and correct the false statements:

Answer

1. True
2. True
3. False. Although all major browsers have private browsing settings, including hiding user browsing history from other users on the same computer, the prevalent belief that "incognito mode" hides user identity and browsing history from Internet service providers, governments, and advertisers is incorrect. This mode only clears the history of their system, and its benefit is limited to hiding search details when using a public computer.
4. True
5. False. They enable users to classify data in clear columns, rows, and sections that facilitate reading and understanding.

6. False. Project management tools
7. True
8. True
9. True
10. False. They are unauthorised programs, illegally copied for distribution or sale without the owner's authorisation.
11. False. Using pirated programs leads to legal consequences, such as fines or even imprisonment in some cases.
12. False. Reading them carefully is required, as unlicensed programs or programs containing viruses can be found even on official stores.

Question

Exercise Three: Fill in the appropriate term

Answer

1. Incognito mode
2. Word processor
3. Remote conferencing programs
4. Project management tools
5. Internet piracy

References

1. Computer program. Follow link: https://www.britannica.com/technology/computer-program
2. How Unlicensed Software Can Compromise Your Data. Follow link: https://www.bluechipit.com.au/how-unlicensed-software-can-compromise-your-data/
3. What is a web browser?. Follow link: https://www.mozilla.org/en-US/firefox/browsers/what-is-a-browser/
4. What are Cookies?. Follow link: https://www.kaspersky.com/resource-center/definitions/cookies
5. What Is Video Conferencing Software?. Follow link: https://www.bigcommerce.com/glossary/video-conferencing-software/
6. Katie Terrell Hanna, spreadsheet. Follow link: https://www.techtarget.com/whatis/definition/spreadsheet
7. Deepak Palasamudram, What is Project Management?, Dec 2022. Follow link: https://2u.pw/RYVwfkV4
8. What is Software Piracy?. Follow link: https://www.javatpoint.com/what-is-software-piracy
9. Software Piracy Facts. Follow link: https://hypertecsp.com/knowledge-base/software-piracy-facts/

10. Investigation: WannaCry cyber attack and the NHS 27 October 2017 https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs

11. What is Pirated Software?. Follow link: https://cyberpedia.reasonlabs.com/EN/pirated%20software.html

12. Devin Partida, Why You Shouldn't Use Pirated Software (But Why People Still Do), 2020. Follow link: https://www.computer.org/publications/tech-news/trends/why-you-shouldnt-use-pirated-software

13. Don't Risk It: The Top 10 Dangers of Downloading Unverified Software, March 2023. Follow link: https://www.lockwell.co/blog/don-t-risk-it-the-top-10-dangers-of-downloading-unverified-software

14. Lital Asher-Dotan, What is the Conficker worm. Follow link: https://www.cybereason.com/blog/what-is-the-conficker-worm

15. How Unlicensed Software Can Compromise Your Data. Follow link: https://www.bluechipit.com.au/how-unlicensed-software-can-compromise-your-data/

16. Raja Viswanathan, Remote work, pirated software, and local admin rights: A deadly cocktail. Follow link: https://www.securden.com/blog/pirated-software-malware.html

17. Do You Know How To Spot Fake Software And Updates? Learn The 7 Red Flags!. Follow link: https://www.alvareztg.com/do-you-know-how-to-spot-fake-software-and-updates-learn-the-7-red-flags/

18. Clare Stouffer, Are you accidentally pirating software? ,January 2024. Follow link: https://us.norton.com/blog/malware/accidentally-pirating-software

19. How to check if a file is safe to download. FOLLOW LINK: https://www.microsoft.com/en-us/edge/learning-center/how-to-check-if-a-file-is-safe-to-download?form=MA13I2

20. Microsoft Defender SmartScreen. FOLLOW LINK: https://learn.microsoft.com/en-us/windows/security/operating-system-security/virus-and-threat-protection/microsoft-defender-smartscreen/

21. How Can I Tell If a Download Is Safe?. FOLLOW LINK: https://codesigningstore.com/how-to-tell-a-download-is-safe

الوكالة الوطنية للامن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative