

COSC130

Fundamentals of Cybersecurity and Privacy

LECTURE 7: HOW TO PROTECT YOURSELF FROM MALWARE, SOCIAL ENGINEERING AND IDENTITY THEFT

How to Protect Yourself from Malware, Social Engineering and Identity Theft

1. Malware
2. Buffer Overflow
3. Social Engineering and Phishing
4. Identity Theft

Much of this lecture is based on

1. Week 3 Malware
Week 7, Section 1 Identity Theft
OpenLearn. *Introduction to Cyber Security*, 2016.
2. Section 2.5 Malware Threats and Solutions
Section 2.6.1 Case Studies: Buffer Overflows
Markus et al. (Eds.), *The ethics of cybersecurity* (Vol. 21). Champaign, IL: Springer.
3. Chapter 21 Malicious Software, W. Stallings. (2017) *Cryptography and Network Security: Principles and Practice*, Global Ed, Pearson.

In-text references to these sources are typically omitted for readability.

How to Protect Yourself from Malware

What is malware?

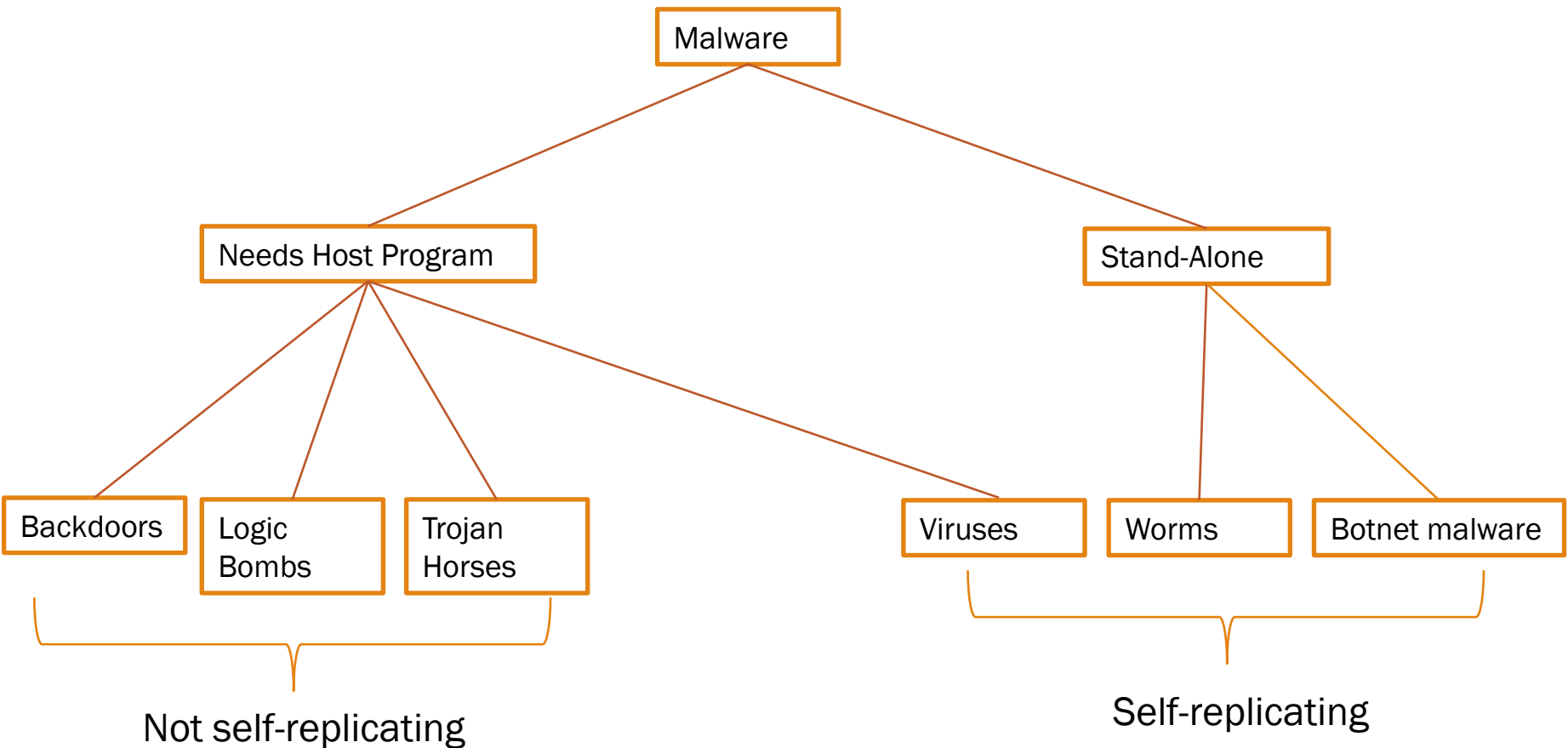
‘Malware’ is short from ‘Malicious Software’. As its name suggests, it is software designed to cause harm to computer resources (including data), usually for financial gain.

Examples of malware include:

- 1) viruses – self-replication, need a host program
- 2) worms – self-replicating, stand-alone code
- 3) Trojan (horses) – not self-replicating; disguises itself as other useful software (e.g., screensaver)
- 4) ransomware – typically encrypts all your data and demands payment to decrypt it
- 5) adware – shows ads to the user
- 6) spyware – records and transmits activities of the users (e.g., passwords)
- 7) botnet malware – enables the attacker to control infected computers and, for example, use them to launch attacks such as denial-of-service attack

Malicious Software

[Stallings, 2017]



Backdoor (Trapdoor)

[Stallings, 2017]

A backdoor, also known as a trapdoor allows access that bypass access control.

While the program is being developed, it is a common practice to use a backdoor to speedup the development and testing.

If the backdoors are not removed before the software is released, they can pose a security vulnerability.

It is not easy to block backdoors in operating system.

Logic Bomb

[Stallings, 2017]

Logic bombs are types of malware that dormant until some specific conditions are met, for example:

- presence or absence of certain files
- particular point in time
- particular user

Trojan Horse

[Stallings, 2017]

Name inspired by the Trojan horse used to sneak in Greek soldiers into Troy.

The malicious code is embedded into another useful or attractive software such as games, software upgrade, screensavers, etc.

Its payload can be to spread virus or a worm, to install a backdoor, delete data, etc.

Zombie

[Stallings, 2017]

“Zombie” or botnet malware is a software that is used to take over another computer on the network.

Botnet refers to a large group of zombie computers that are controlled by the attacker and can be used launch distributed denial of service (DDoS) attacks.

Virus Structure

[Stallings, 2017]

Viruses typically have the following components:

- infection mechanism - enables replication
- trigger - event that makes payload activate
- payload - what it does, malicious or benign

Viruses can be embedded in the other code at the beginning (prepended), at the end (postpended) or somewhere else (embedded).

When the infected program gets executed, the virus gets executed first, and then the original code.

Viruses

[Stallings, 2017]

Viruses typically have some or all of the following phases:

- dormant phase – waiting on trigger event
- propagation phase – replicating/spreading
- triggering phase – triggered by some event to execute its payload
- execution phase – execution of payload

A Simple Virus Structure

[Stallings, 2017]

```
Program V :=
{goto main;
 1234567;

  subroutine infect-executable :=
    {loop;
      file := get-random-executable-file;
      if (first-line-of-code = 1234567)
        goto loop
      else prepend V to file;}

  subroutine do-damage :=
    {whatever damage is to be done}

  subroutine trigger-pulled :=
    {return TRUE if some condition is met}

main:   main-program :=
        {infect-executable;
        if (trigger-pulled)
          do-damage;
        goto next;}

next:
}
```

Compression Virus [Stallings, 2017]

When a virus gets prepended to a program, the file gets bigger. This change in size can be used to detect viruses.

To counter that, compression viruses compress a file first and then prepend a copy of itself. When the file is executed, the original portion of the file gets de-compressed and then executed.

```
Program CV :=
  {goto main;
   01234567;

   subroutine infect-executable :=
     {loop;
      file := get-random-executable-
file;
      if (first-line-of-code = 1234567)
        goto loop
      else
        {compress file;
         prepend V to file;}}

main:  main-program :=
       {infect-executable;
        uncompress the original file;
        execute original file;}
}
```

Types of Viruses [Stallings, 2017]

Parasitic virus: “Traditional and still most common form of virus, it attaches itself to executable files and replicates when the infected program is executed.”

Memory-resident virus: “Lodges in main memory as part of a resident system program, and infects every program that executes.”

Boot sector virus: “Infects a master boot record and spreads when a system is booted from the disk containing the virus.”

Stealth virus: “A virus explicitly designed to hide itself from detection by antivirus software.”

Polymorphic virus: “Mutates with every infection, making detection by the “signature” of the virus impossible.”

Metamorphic virus: “Mutates with every infection, rewriting itself completely at each iteration changing behavior and/or appearance, increasing the difficulty of detection.”

How to Protect Yourself from Malware [Markus et al., 2020]

How does malware spread?

In the past, malware typically spread through floppy-disks that were shared between users (e.g., in the office).

Nowadays, some viruses still infect files are spread via USB sticks (flash drives).

However, majority of malware is now spread via the Internet:

- Email attachments – need to trick users into opening it, usually via social engineering, similar to fishing and spear fishing
- Drive-by-download – tricks users into visiting a website designed to exploit a vulnerability in the browser (for example, a buffer overflow) and execute the malware payload
- Malvertising – inserting malware into ads
- Waterholing – like spear-phishing, requires knowledge about the victim (usually an organisation), what websites they visit or what servers they use for software updates, etc, then compromising these websites

How to Protect Yourself from Malware

What are typical malware payloads?

In the past, malware typically aimed at corrupting computer resources, e.g., by deleting files or preventing the system from booting.

Nowadays, the most common payloads include:

- Encrypting the files and requesting payment for decrypting them (ransomware)
- Keyloggers to obtain login details and other data
- Remote control tools
- Controlling large number of computers (botnets)

How to Protect Yourself from Malware

Infamous malware attacks

- ❑ 2003: SQL Slammer worm that infected more than 75,000 hosts over the Internet
 - Exploited buffer-overflow vulnerability in Microsoft SQL Server
 - Exposure: infected servers were not protected by a firewall
- ❑ 2017: waterholing attack where an infected update for the CCleaner tool was delivered to 700,000 customers

How to Protect Yourself from Malware

How to Protect Yourself from malware?

Install an anti-malware software. Some of the well known ones include:

- 1) Bitdefender Antiviris Plus
- 2) Norton Antivirus Plus
- 3) ESET NOD32 Antivirus
- 4) G Data Antivirus
- 5) Malwarebytes Premium
- 6) Webroot AntiVirus
- 7) F-Secure Anti-Virus
- 8) Trend Micro Antivirus + Security
- 9) Kasparsky Premium
- 10) Sophos Home Premium

Useful Links:

Sophos Threatsaurus (pdf) includes glossary on malware terms, as well as practical hints and tips on how to protect yourself online https://ugc.futurelearn.com/uploads/files/3f/d3/3fd36a66-d941-4595-b587-1a7b41998ae9/Week_3_Sophos_Threatsaurus_AZ.pdf

Buffer Overflow

[Markus et al., 2020]

What is buffer overflow?

Buffer overflow is a vulnerability in software applications that can be exploited to launch various attacks.

In order to run a program and execute computation, usually require some space in the main memory. A buffer is a block of main memory with specified location and size.

In some programming languages, programmers are in charge of allocating the size to buffers so that they can hold all the data they are supposed to hold. Such programming languages are not considered 'memory safe'.

If a buffer is too small, the program will read from/write to adjacent buffers. An attacker can exploit this vulnerability to execute arbitrary commands and breach security services.

Buffer Overflow [Markus et al., 2020]

```
1 #include <stdio.h>
2 void main(void) {
3     int privilege_level = 1;
4     char buf[124];
5     fgets(buf, 1024, stdin);
6     if(privilege_level > 10) {
7         printf("You have admin rights. Level: %d\n",
8             privilege_level);
9     }
10    printf("Your input was: %s\n", buf);
11 }
```

Prevention Techniques

1. Data Execution Prevention (DEP)
2. Address Space Layout Randomization (ASLR)
3. Stack Canaries
4. Control-Flow Integrity (CFI)
5. and so on

Phishing

What are (arguably) the worst vulnerabilities that are hard to patch?

One of the worst vulnerabilities are those based on human factor.

How can 'human factor vulnerabilities' be patched?

The best way to alleviate the 'human factor vulnerabilities' is through raising cybersecurity awareness and training.

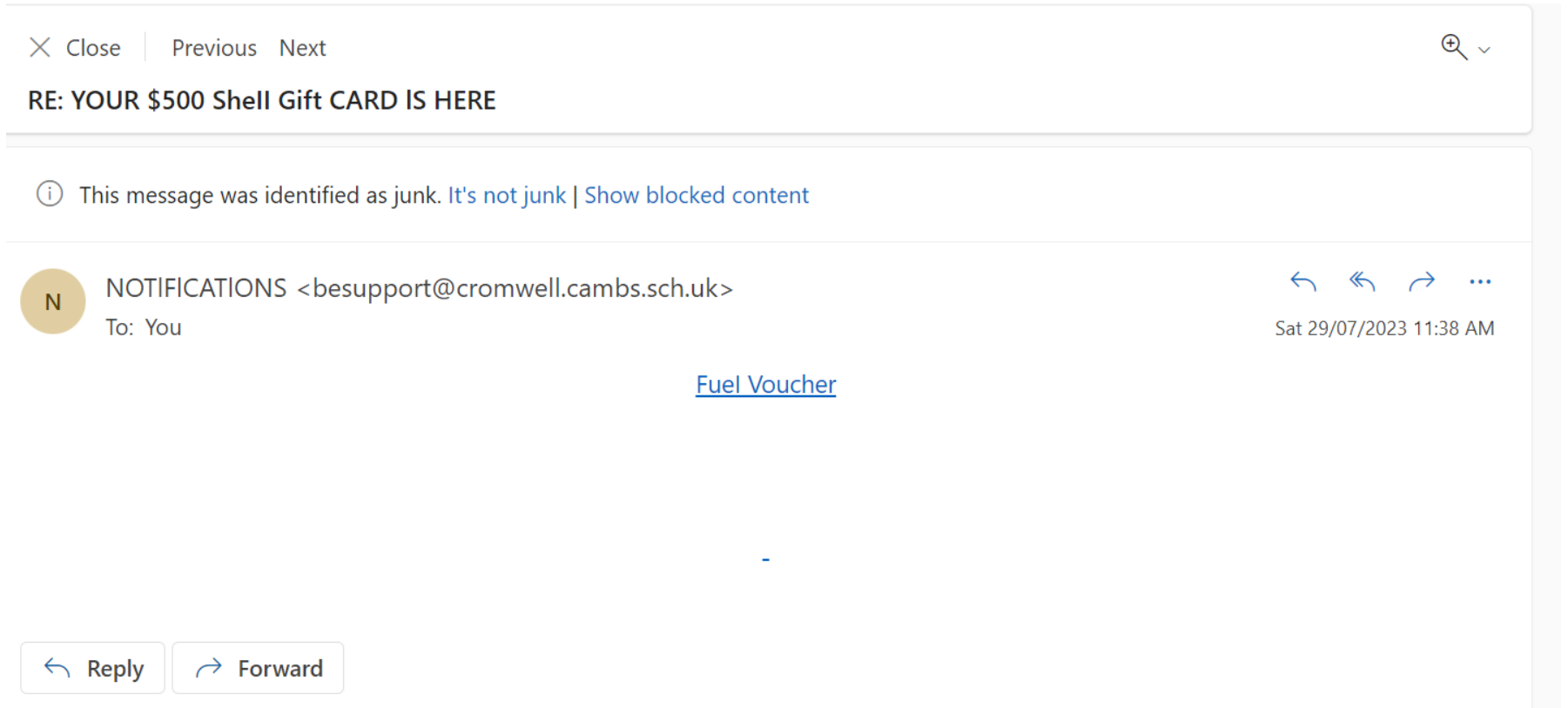
What type of attacks can exploit human factor vulnerabilities?

'Social Engineering' is a suite of attacks that exploits people's generosity/good will/trust/fear/gullibility/greed/etc. Phishing is a form of social engineering.

For example, an attacker may pretend to be an heir due to inherit a large sum of money but has no account that the funds can be deposited into. He offers his victim a substantial percentage of the sum for using that person's account.

As another example, an attacker may send an email pretending to be a bank officer informing the victim that their bank account will be closed unless they use the link provided to confirm their login details.

Phishing Examples



<https://determinations.libfoobar.com/V4ANtrUQiaxOCgsxnnHg2HWi9eHjn9qIbgg>

Phishing Examples

✕ Close | Previous Next



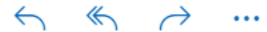
Re: About Charitable dispositions - 31/07/2023

This message was identified as junk. We'll delete it after 10 days. [It's not junk](#)



Sara Hoppitt

To: Recipients



Tue 1/08/2023 3:34 PM

Hello ,

Compliment of the day. My name is Sara Hoppitt. I am a philanthropist. I dedicate my time and resources towards uplifting the downcast in different parts of the world. I am 68 years of age, and I was diagnosed with cancer about a year ago. All efforts to fight and resist it has proved abortive and as such, I am left with no other option than to give out financial donations to people that are inclined with charitable dispositions, so that they can also reach out to the less privileged in their immediate environment: especially those that are most affected by the Covid-19 pandemic. I have therefore bequeathed part of my fortune (Total sum of £1,963,920.00 Great Britain Pounds) to you in cash for your personal and charitable goals. I know I have never met you in person, but instincts tell me to do this in good faith and I hope you act sincerely. Reply for more details if interested.

Please note that this is solely a charity donation to you, for your personal and charitable goals. I hope you can reach out to the less privileged in your immediate environment.

Best Regards,
Sara Hoppitt



Reply



Forward

Phishing Examples

✕ Close | Previous Next



Limited Offers!

ⓘ This message was identified as junk. We'll delete it after 10 days. [It's not junk](#) | [Show blocked content](#)



Your Harbor Freight Reward <xpgyzehuhv@meta-town.net>
To: You



Tue 1/08/2023 3:26 PM

HARBOR FREIGHT
QUALITY TOOLS LOWEST PRICES

08-01-2023

Dear Harbor Freight Good Shopper,

We would like to offer you a unique opportunity to receive a brand new **170 PIECE STANLEY TOOL SET!**

To claim it, simply take this short survey about your experience with us.

Your opinion is very valuable.



GET STARTED NOW!

Share your dining experience, and we'll present you with a delightful surprise.

Regards,
Your Harbor Freight Rewards Team

If you no longer wish to receive these emails, you may unsubscribe by clicking [here](#) or by writing to 9101 W. Sahara Ave, Las Vegas, NV 89117

← Reply

→ Forward


Phishing Examples

✕ Close | Previous Next



Survey Response Confirmation.

ⓘ This message was identified as junk. We'll delete it after 8 days. [It's not junk](#) | [Show blocked content](#)

 CashApp <gykzqqht@meta-town.net>
To: You

⏪ ⏩ ⏴ ⏵ ⋮

Sun 30/07/2023 2:43 PM

Cash App

Dear Ibrankov,

We are excited to extend an invitation to you for sharing your Cash Survey purchase experience to help our services for valued customers like yourself. As a token of our appreciation, we present you with an exclusive opportunity to receive a promotional reward valued at \$90 or more. Simply take a few moments to complete this brief survey, and the reward will be yours to enjoy.



Start Now!

Regards,
CashApp Team

If you no longer wish to receive these emails, you may unsubscribe by clicking [here](#) or by writing to 9101 W. Sahara Ave, Las Vegas, NV 89117

Phishing Examples

✕ Close | Previous Next



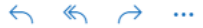
RE: You are at RISK!!

ⓘ This message was identified as junk. [It's not junk](#) | [Show blocked content](#)



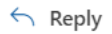
Internet Security <besupport@cromwell.cambs.sch.uk>

To: You



Fri 28/07/2023 10:59 AM

[VIRUS Detected On Your Device!](#)



Reply



Forward

Phishing Examples

✕ Close | Previous Next



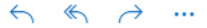
RE: Package delayed because....

 This message was identified as junk. [It's not junk](#) | [Show blocked content](#)



AUpost-Service <info@sdm.be>

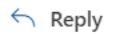
To: You



Thu 27/07/2023 12:36 PM

[Confirmation Of Address Required](#)

-



Reply



Forward

Phishing Examples

✕ Close | Previous Next



We have reserved (1) DeWalt Drill exclusively for you.

⏏ This message was identified as junk. We'll delete it soon. [It's not junk](#) | [Show blocked content](#)

BR Bunnings Reward <iloEpFi@christianamzwaro.click>
To: You

⏪ ⏩ ⏴ ⏵
Wed 19/07/2023 7:06 AM



Congratulations! You've Won a DeWalt Drill from Bunnings!



We hope this email finds you well! We are delighted to inform you that as a highly valued and loyal customer of Ace Hardware

We understand that there are many scams and spam emails out there, but we assure you that this is not one of them. You were selected through a random drawing and have been verified as a legitimate winner.

CLAIM REWARD


Phishing Examples

✕ Close | Previous Next



Verify your wallet

ⓘ This message was identified as junk. We'll delete it after 2 days. [It's not junk](#)

 Coinbase <user@creditmaven.remiahhosting.com>
To: You

⏪ ⏩ ⏴ ⏵
Mon 24/07/2023 8:38 PM

Our system has shown that your Coinbase wallet has not yet been verified. This verification can be done by clicking the button below. All wallets must be updated before **July 31, 2023**.

Verify your wallet

*For further assistance with this issue, please
contact our support team [here](#).*

[Terms of service](#)

Coinbase since 2012

Identity Theft [OpenLern, 2016]

What is identity theft?

Identity theft is a type of cybercrime where an attacker steals sufficient amount of personal information to impersonate the victim to open credit cards or take loans in victim's name, get various government benefits and identity documents such as driver's licenses or passports with the victim's identity but another person's photo.

How is identity theft done?

In the traditional physical world, identity theft was typically committed by intercepting official letters to learn personal details, including names, addresses and bank accounts.

In the online world, attackers typically resort to using malware to collect personal information from the victim's computer, phishing attacks to trick a victim into revealing their personal information and stealing large databases with personal information from big companies.

Identity Theft

What type of information are cybercriminals looking to steal?

- Name and address
- Date and place of birth
- Driver's licence number
- Passport details
- Mother's maiden name
- Credit card details and pin number
- Tax File Number
- Medicare card details
- Online accounts login details

Identity Theft

What are the consequences of identity theft for the victim?

The victims of identity theft typically have hard time proving that credit cards and loans were opened in their name by an attacker and not by them. It may take years to prove this and during that time many victims endure a great deal of suffering.

How to prevent identity theft?

While identity theft cannot be fully prevented, the risk can be greatly reduced by:

1. Running up-to-date antimalware software
2. Running latest updates of software you use on your devices (they will have fewer vulnerabilities than the older versions)
3. Using strong passwords and, where possible, two-factor authentication
4. Avoid using public Wi-Fi
5. Not sharing personal information online and using strict security and privacy settings in your browser and social networks
6. Being aware of social engineering and especially phishing – as a rule, never disclose your personal information via email or to strangers; only update personal information through official websites of banks, etc.

Identity Theft

How to detect identity theft?

- Somebody is purchasing goods with your money - you receive bills or bank statements showing purchases you did not make, or your credit card gets declined.
- You receive bank statements for loans or credit cards you did not applied for
- You receive a statement about a government benefit that you never applied and are not receiving.
- You are refused credit due to a poor credit record you know nothing about.
- You are contacted by debt collectors.

References

[**OpenLern, 2016**] OpenLern. *Introduction to Cyber Security*, 2016.

[**Markus et al., 2020**] Markus, C., Gordijn, B., & Loi, M. (2020). C. Markus, B. Gordijn, & M. Loi (Eds.), *The ethics of cybersecurity* (Vol. 21). Champaign, IL: Springer.

[**Stallings, 2017**] W. Stallings. (2017) *Cryptography and Network Security: Principles and Practice*, Global Ed, Pearson.