



Cyber Crimes Task

[Visit our website](#)

Introduction

The bootcamp you are starting today is structured as a series of “tasks”. Tasks include a lesson component designed to teach you the theory needed to develop your skills, as well as a practical component designed to give you the opportunity to apply your newly gained knowledge by completing practical exercises.

This task serves as an introduction to the field of cybersecurity, emphasising information security and various types of cyber-attacks, along with the methods used to carry them out. Cybersecurity is part of everyday life and an increasing concern for businesses of all sizes, whether you are aware of it or not. At the end of this task, you will have an opportunity to engage with a typical cyber-attack and explore how your data may have been breached.

What is cyber security?

As you well know, our daily activities have extended beyond physical space into cyberspace. These days, conducting business, communicating with others, and sharing information often occurs virtually. Unfortunately, the convenience of operating in cyberspace is tainted by cybercrime, cyberterrorism, and even cyber warfare. These negative activities necessitate cyber security.

The field of cyber security is broad and may be described in different ways depending on the context. In general, it can be described as the processes used to protect computers, networks, and programs from unauthorised access or attacks intended to harm an individual or organisation. Harm is often related to financial loss or data privacy breaches. In the case of organisations, financial loss may occur due to a cyber-attack halting or subverting operations within the business. The overall economic loss attributed to cybercrime is estimated at \$600 billion annually, nearly one percent of global gross domestic product (GDP), according to a report by [**CSIS and McAfee**](#) (2018).

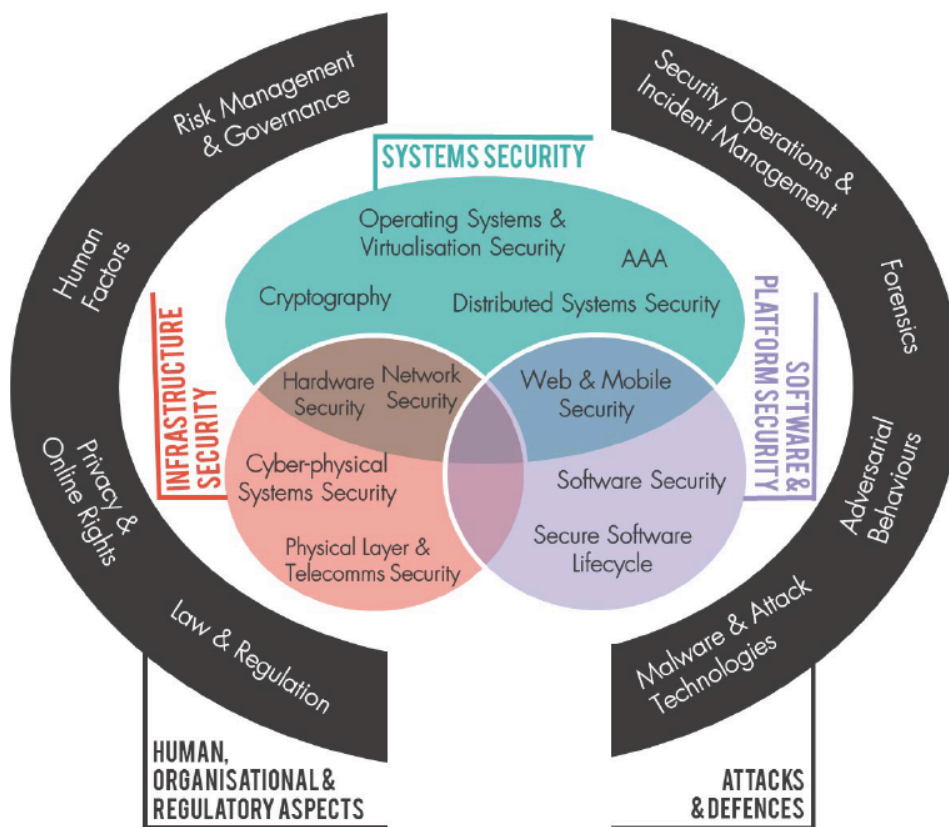
Cyber security categories

Cyber security can be split into three broad categories: systems, software and platform, and infrastructure security. Most cyber security professionals focus on niche areas within one of these categories. However, some aspects of each of the areas may overlap. For example, web network security falls under systems and infrastructure security.

Systems security includes elements such as firewalls, encryption, and passwords. Software security refers to using the best coding practices to prevent bugs that may lead to vulnerabilities, which includes web and mobile applications. Infrastructure security consists of network and hardware security as well as cyber-physical and physical security. The three types of cyber security are all associated with two more general topics:

1. human, organisational, and regulatory aspects; and
2. methods of attack and defence.

The relationships between all the spheres of cyber security are summarised in the following diagram:



The 21 Knowledge Areas (KAs) in the CyBOK Scope (Martin et al., 2021, p. 4)
CyBOK Version 1.1.0 © Crown Copyright, The National Cyber Security
Centre 2021, licensed under the [**Open Government Licence**](#)

CIA triad

A foundational part of cyber security is information security, which is defined as the conservation of **c**onfidentiality, **i**ntegrity, and **a**vailability (CIA) of information. These three key concepts, known as the CIA triad, provide guidance for defending against threats and detecting problems (Samonas & Coss, 2014). Traditionally, information security has centred around technical controls, however, these days there is a need to include social and human factors in security management (Samonas & Coss, 2014). This has led to broadening the original definitions of the CIA triad.

Confidentiality conservation involves protecting against the risk of unauthorised access and leaking of information. A modern concern in this area is personal or proprietary information, especially sensitive data related to a person's health or finances. The meaning of integrity in the triad has grown beyond protecting information from unauthorised modification. It now also involves addressing several social-technical issues such as authenticity, **non-repudiation** (proof of delivery and receipt), responsibility, ethicality, the moral integrity of people, and trust. Availability was traditionally only related to preventing unauthorised access that denied illegitimate users from accessing and modifying information. These days it also refers to creating systems that promote security while maintaining efficiency. Given the choice, users will prioritise convenience over security so cyber security professionals need to find a balance between the two to minimise a user's vulnerability to cyber-attacks.

Cyber-attacks

The motivation behind a cyber-attack is not always financial. Some individuals or organisations have political agendas and others seek to harass people they know or want to sabotage previous employers.

Crimes that could be committed without technology but are made easier by the use of technology are labelled as "cyber-enabled". These include offences such as cyberbullying, **doxing** (release of private information), or **advance-fee fraud (419 scams)** are a subset of this category.



Extra resource

Have you heard about **scam baiting**? This is the practice of wasting a scammer's time or resources to reduce the number of victims of scams. Explore YouTube channels such as **Scammer Payback**, which in some cases aid authorities in identifying the scammers.

Cyber-dependent attacks are varied and may be carried out by criminals, activists, and states. These types of attacks are usually facilitated by **malware** (malicious software). Crimes with a financial goal that are cyber-dependent include:

- **Email spam:** Unsolicited bulk emails sent to entice people to buy fake products.
- **Phishing:** A subset of spam email where victims are persuaded that the email is from a legitimate source and then provide login credentials for their online banking, social media, or email accounts. Sometimes phishing emails are targeted towards a specific individual or organisation, making them more believable. This is known as "spear" phishing.
- **Financial malware:** Records credit card credentials or usernames and passwords when a user visits a website of interest to criminals. These credentials may be sold to other cybercriminals.
- **Click fraud:** Bots are used to click on web adverts to defraud advertisers.
- **Unauthorised cryptocurrency mining:** Computers are infected with malware to mine cryptocurrency. Webpages can also be infected with scripts that use visitors' computers to mine.
- **Ransomware:** Users' files are encrypted and held for ransom using malware.
- **Denial of service (DoS):** Server bandwidth is consumed to slow down or disable a system via the network. Although this can sometimes happen legitimately when a site is overwhelmed by traffic after being linked to by a site with a larger audience, it can also be deliberately engineered in a number of ways. A subset of DoS attacks is a distributed DoS (DDoS) where multiple connected online devices (a botnet) flood a target website with traffic. DDoS attacks are particularly dangerous because they can overwhelm the target with a high volume of traffic from numerous sources, making it difficult to mitigate.
- **Man-in-the-middle attack:** A conversation or data transfer is intercepted. This allows an attacker to access confidential information or insert malware.

(Stringhini, 2021, pp. 229–232)

At the heart of cybercrime is the management of digital identities and personally identifying data. An ideal scenario would be where identities and data are protected without enabling criminals or terrorists to hide behind privacy policies (Samonas & Coss, 2014).



Extra resource

Explore a database of real [email phishing examples](#) to identify common characteristics of phishing emails.

Malware

As mentioned, malware is responsible for a large proportion of cyber-attacks. There are several types of malware that can be grouped according to six categories.

1. Standalone or dependent

Worms or **botnets** are examples of malware that are standalone, meaning they are a complete program that will run once executed. Viruses and malicious browser plug-ins require a host program. Viruses typically insert instructions into the program so that the malware is executed along with the legitimate program. It is usually easier to detect standalone programs.

2. Persistent or transient

Most malware is persistent, meaning it is embedded somewhere in the file system. However, some malware resides in memory. This transient malware is difficult to detect using antivirus software as the malware disappears when the system is rebooted.

3. Layer of the system

Persistent malware can be installed and run at different layers of the system. Malware on the deeper layers, such as firmware or the boot sector, is more difficult to detect than malware that affects drivers or application programming interfaces (APIs).

4. Automatic or activated

Auto-spreading malware installs and runs itself while other malware requires a user to execute it. Users usually do this accidentally by clicking on a link or email attachment.

5. Static or dynamically updated

Traditionally malware was static. However, attackers are creating more sophisticated malware that can evade detection techniques by updating via a malware server.

6. Individual or coordinated network

Individual malware tends to be designed to target a specific victim whereas coordinated networks (botnets) are used for distributed denial of service (DDoS), spam, or phishing to a mass audience.

(Lee, 2021, pp. 202–204)



Extra resource

Read about [Stuxnet](#), which was used to sabotage Iran's nuclear fuel enrichment program, and the [ransomware attack](#) that caused a shutdown of a major US fuel pipeline. How would you categorise Stuxnet and ransomware according to the six categories?

A type of software that falls in a grey area between legitimate software and malware is a potentially unwanted program (PUP). This software is usually downloaded as part of a program such as a free version of a mobile game app. PUPs often come in the form of adware to collect data on users who have in theory agreed to this via the terms and conditions of download. Since PUPs have the potential to become malware, they are also classified as such from a cybersecurity perspective.

The mechanisms used to spread malware are related to whether the malware spreads automatically or needs to be activated. System vulnerabilities provide loopholes and backdoors for malware to infect a system automatically. Smart devices and [Internet of things \(IoT\)](#) devices may also be used as access points to infiltrate a system.

Alternatively, malware is activated by a person, and there are many avenues for malware to be activated by humans. Some of the most popular methods used to make this happen include:

- Downloading infected files via email attachments, websites, or file-sharing sites.
- Clicking on links to malicious websites, where the link may redirect to an unexpected webpage (known as a URL redirection).
- Visiting a compromised site where a virus hidden in the HTML downloads automatically as the webpage is loaded.
- Inserting infected external hard drives or USB devices.
- Succumbing to social engineering attacks where a user is deceived into providing sensitive information or downloading malware.

Being aware of these methods can help to prevent cyber-attacks in a personal capacity as well as at an organisational level. Social engineering in particular requires you to be aware of the tactics used by cyber criminals to deceive you. One tactic is to get you into a heightened emotional state such as being fearful or excited. This is because you are more likely to make rash decisions in a heightened (positive or negative!) emotional state. They will also employ elements of urgency and trust to entice you to make a decision without thinking carefully because the data seems to come from a trusted source (Kaspersky, n.d.).

Although malware often leaves no sign of its presence, it is also a good idea to be aware of the anomalies that may indicate an infection. One of the most common signs is reduced computing performance such as slow-running processes, random programs running in the background, and applications taking a long time to load. Other signs include a different homepage on your browser or pop-up adverts occurring more frequently than usual. In the worst-case scenario, your computer may crash completely. For (DDoS) attacks, detection is based on analysing the statistical properties of the traffic, for example, the number of requests sent to the network server over a short time frame.

If you suspect a device may have malware, the first step is to scan the system with an antivirus tool. Common antivirus programs include **proprietary tools** by Norton, Bitdefender, and McAfee. While many antiviruses may promise the best security, you should also consider the real malware detection rates of the antivirus. When choosing an antivirus program it is also important to consider your needs as programs often come with additional features such as password management, safe browsing extensions, or parental controls. Some antivirus programs are available for free, such as Avast One Essential, but these usually only include basic features. If you have an antivirus installed, it will periodically scan your system for malware, however, it may not detect an attack, as malware is often designed to evade antivirus applications. So, it is important to update your antivirus software often.



Extra resource

Learn more about malware and attack technologies in [Malware & Attack Technologies](#), published by *The Cyber Security Body of Knowledge*.

In the following practical tasks, you will answer questions related to data breaches and social engineering via email. Ensure that you save the practical task files in this task's folder before requesting a review.



Practical task 1

Follow these steps:

- Use [Have I Been Pwned](#) to identify if any data related to your email address has been part of a data breach.
 - Explore the data breaches where your data was exposed to the public or look at some of the largest breaches at the bottom of the webpage.
 - Create a text file called **data_breach.txt** in this task's folder to answer the following questions.
 - What do you think the risk is for individuals when their email addresses and passwords are exposed to the public?
 - Name two actions you can take to protect yourself against the risks associated with data breaches.
-



Practical task 2


Imagine you are at work when you get the following email from your bank.

Subject: URGENT - complete forms
From: Fraud Team <frud_servces@bank.com>

Hello,

We have detected several incorrect attempts to sign in to your online banking profile. Please fill in the attached forms to temporarily freeze your account as soon as possible.

Thanks,
Fraud Team

 **Fraud forms.zip**

You skim-read the email as you are very busy with several looming deadlines. It seems legitimate and you open the zip folder to quickly fill in the form as you are worried about the security of your online banking profile. When you open the PDF file in the folder you realise that this is not a legitimate form from your bank. Annoyed by your time being wasted, you mark the email as spam and continue with your day. Later that day your computer seems to be slower than usual. You assume it is because you have several browser tabs open even though you don't usually have this problem.

A few days later after a cyber security training session, you realise you should read your emails more carefully.

Create a new text file called **email_security.txt** in this task's folder. Then, answer the following questions:

- What three things should have alerted you to the fact that the email from the bank was not legitimate?
- Do you think it is possible your computer is infected with malware based on the given email scenario? Justify your answer. (Hint: Think about a possible mechanism of infection.)
- Write a paragraph to train fellow employees on phishing, social engineering, and how to avoid malware infection (200–400 words).

Important: Be sure to upload all files required for the task submission inside your task folder and then click "Request review" on your dashboard.



Share your thoughts

Please take some time to complete this short feedback **form** to help us ensure we provide you with the best possible learning experience.

Reference list

Kaspersky. (n.d.). *What is social engineering?*

<https://www.kaspersky.com/resource-center/definitions/what-is-social-engineering>

Lee, W. (2021). Malware & attack technologies. In A. Rashid, H. Chivers, E. Lupu, A. Martin, & S. Schneider (Eds.), *The cyber security body of knowledge* (1.1.0, pp. 201–222). The National Cyber Security Centre. https://www.cybok.org/media/downloads/CyBOK_v1.1.0.pdf

Martin, A., Rashid, A., Chivers, H., Danezis, G., Schneider, S., & Lupu, E. (2021). Introduction. In A. Rashid, H. Chivers, E. Lupu, A. Martin, & S. Schneider (Eds.), *The cyber security body of knowledge* (1.1.0, pp. 1–16). The National Cyber Security Centre.

https://www.cybok.org/media/downloads/CyBOK_v1.1.0.pdf

Samonas, S., & Coss, D. (2014). The CIA strikes back: Redefining confidentiality, integrity and availability in security. *Journal of Information System Security*, 10(3), 21–45.

<https://www.jissec.org/Contents/V10/N3/V10N3-Samonas.html>

Stringhini, G. (2021). Adversarial behaviours. In A. Rashid, H. Chivers, E. Lupu, A. Martin, & S. Schneider (Eds.), *The cyber security body of knowledge* (1.1.0, pp. 223–250). The National Cyber Security Centre. https://www.cybok.org/media/downloads/CyBOK_v1.1.0.pdf