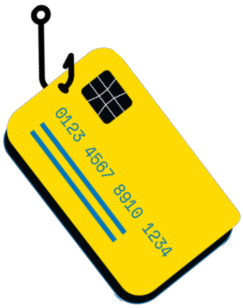

# CYBERSECURITY

**You are an important link in the security chain!**

GHENT
UNIVERSITY

# PHISHING




## Cybercriminals use phishing attacks to trick you into believing an email comes from a trusted source.

If you take the bait, you might unintentionally reveal sensitive information or infect your device with malware, which can lead to a data breach, identity theft, financial loss, or worse.

To keep you alert, the IT security team will periodically send out simulated phishing emails. **Please report any phishing emails** you receive, as this helps us strengthen our detection systems.

---

# RANSOM-WARE

## Ransomware locks files or entire systems and demands a ransom to restore access, which, in the worst case, can impact the whole university.

Entire network drives of research groups can be locked because a single individual fell victim to ransomware.

**Therefore, keep your software and operating system up to date** to prevent attackers from exploiting vulnerabilities to install ransomware.

---

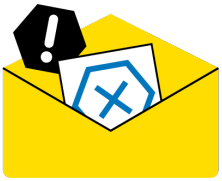
# WEAK PASSWORDS

### (AND REUSING PASSWORDS)

## Weak passwords that are easy to guess or reused across multiple accounts are an easy target for hackers.

If an attacker gets hold of your password, they will exploit it. **Protect your Ghent University account by using a unique and strong password, setting up multiple methods for multi-factor authentication**, and storing passwords in a personal password manager, secured with a long, hard-to-guess password.

# MALWARE



**Malware is a broad term for malicious software, such as viruses, spyware, and trojans, that can infect your devices and steal or destroy your data.**

Malware can steal or modify your files, slow down systems, allow attackers to spy on your activities, or, in the worst case, take full control of your device.

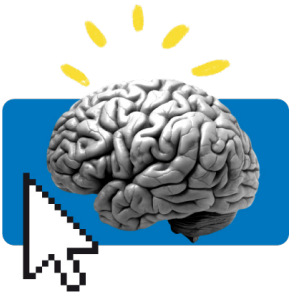
Cracked software or downloads from unofficial websites often contain malware. **Only install legitimate and trusted software**, ideally from the company's official portal or directly from the vendor's website.

# SOCIAL ENGINEERING

**Social engineering is a collection of deceptive techniques that exploit human traits like curiosity, trust, ignorance, greed, and fear.**

Attackers use these techniques to manipulate victims into revealing confidential information or performing fraudulent actions.

Attackers can bypass technical security measures by misleading individuals through deceptive emails or phone calls. **Always verify suspicious emails through a secure second channel, such as a phone call, to confirm their legitimacy**.



# DATA BREACHES


**A data breach occurs when personal or confidential information is accessed, stolen, or disclosed without authorisation.**

Leaked data can be misused or monetised in various ways, potentially harming Ghent University and its staff and students. To keep data secure, **store your data on the platforms supported by the university** and take additional measures where necessary, such as encrypting sensitive data.

# CYBERSECURITY: YOU ARE AN IMPORTANT LINK IN THE SECURITY CHAIN!

Ghent University takes cybersecurity very seriously. We implement numerous high-tech measures, including firewalls, antivirus software, and monitoring systems, to address the many cyber threats we face daily. However, technological measures alone are not enough.

**Your vigilance and common sense are the difference between a secure environment and the risk of data breaches or hacking. This makes you an essential link in our defence strategy.**

## WHAT CAN YOU DO?

### DO YOU NOTICE SOMETHING SUSPICIOUS?

When you notice unusual activity in an application or on a device, **notify the IT helpdesk as soon as possible** at helpdesk.ugent.be/helpme/en.
Quick action can prevent a lot of harm!

### BOOST YOUR KNOWLEDGE!

Cybercriminals are getting smarter, so stay ahead of them! **Follow our online IT security training** at helpdesk.ugent.be/security-training to learn how to recognise and prevent threats.

### KNOW AND FOLLOW THE RULES AND POLICIES

Being well-informed is the key to working securely.
**Read all the guidelines and policies** for working securely at Ghent University at helpdesk.ugent.be/security/en.

**TOGETHER WE CAN MAKE GHENT UNIVERSITY MORE SECURE.
BE ALERT, BE SECURE!**