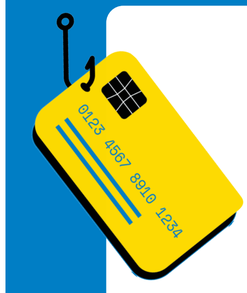
FUNCTIONAL DOMAIN ICT



PHISHING

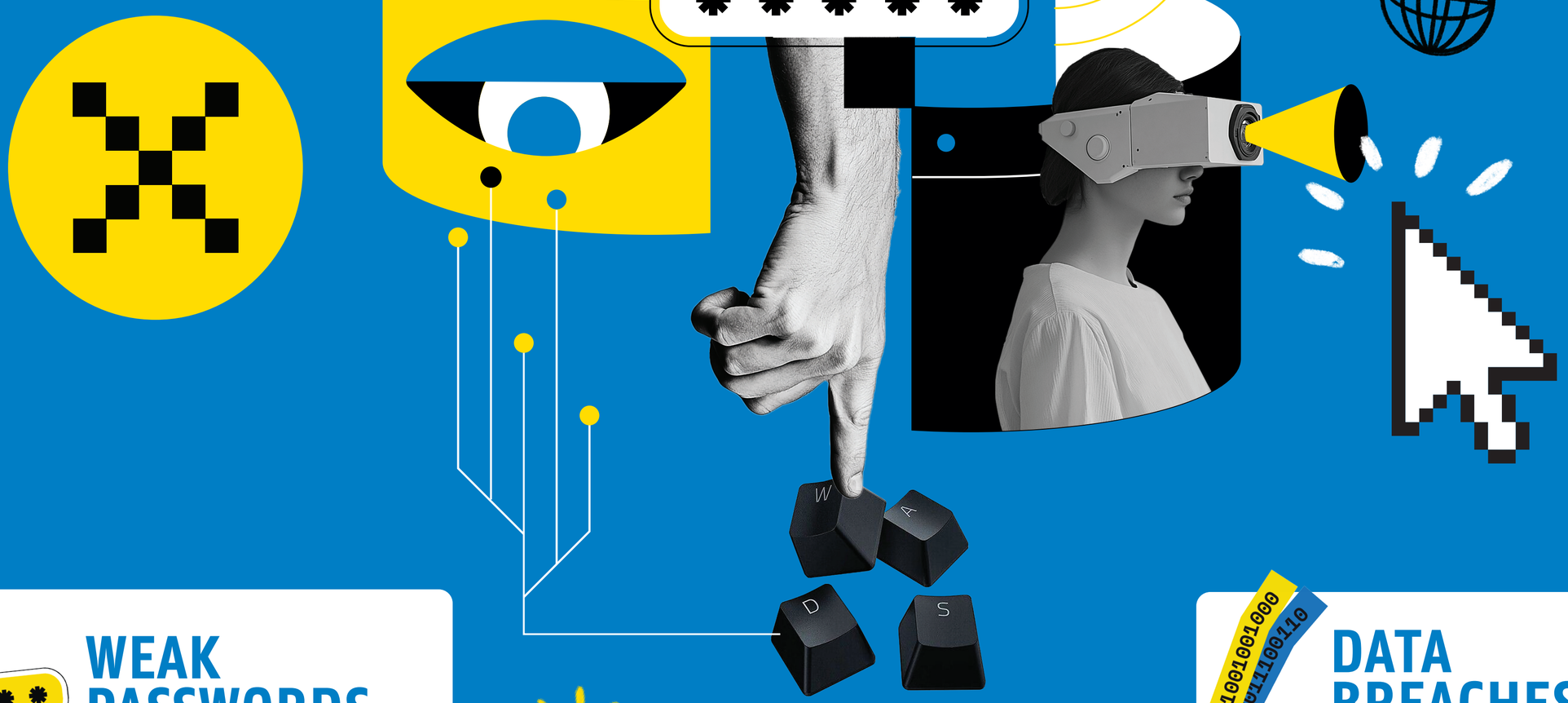
Please report any phishing emails you receive, as this helps us strengthen our detection systems. To keep you alert, the IT security team will periodically send out simulated phishing emails

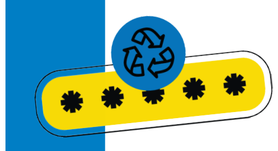
MALWARE

Only install legitimate and trusted software, ideally from the company's official portal or directly from the vendor's website.

RANSOMWARE

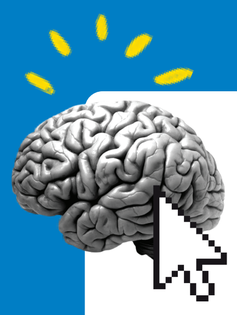
Keep your software and operating system up-to-date to prevent attackers from exploiting vulnerabilities to install ransomware.





WEAK PASSWORDS

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.



SOCIAL ENGINEERING

Always verify suspicious emails through a secure second channel, such as a phone call, to confirm their legitimacy.

DATA BREACHES

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.

STAY AHEAD OF THE NEXT CYBER THREAT

You are an important link in the security chain!

WHAT CAN YOU DO?

DO YOU NOTICE SOMETHING SUSPICIOUS?

Notify the IT helpdesk as soon as possible at
helpdesk.ugent.be/helpme/en

BOOST YOUR KNOWLEDGE!

Follow our online IT security training at
helpdesk.ugent.be/security-training

KNOW AND FOLLOW THE RULES AND POLICIES

Read the guidelines and policies for working securely at
helpdesk.ugent.be/security/en

GHENT UNIVERSITY