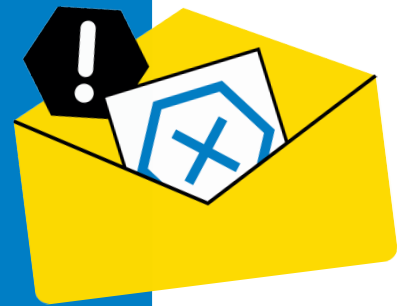




PHISHING

Rapporteer iedere phishing e-mail die je in je inbox vindt, dat helpt onze detectie-systemen. Om je bij de les te houden, stuurt het IT-security team je periodiek een simulatie phishing e-mail.



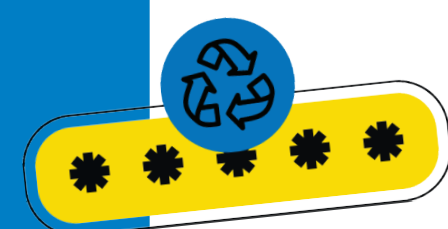
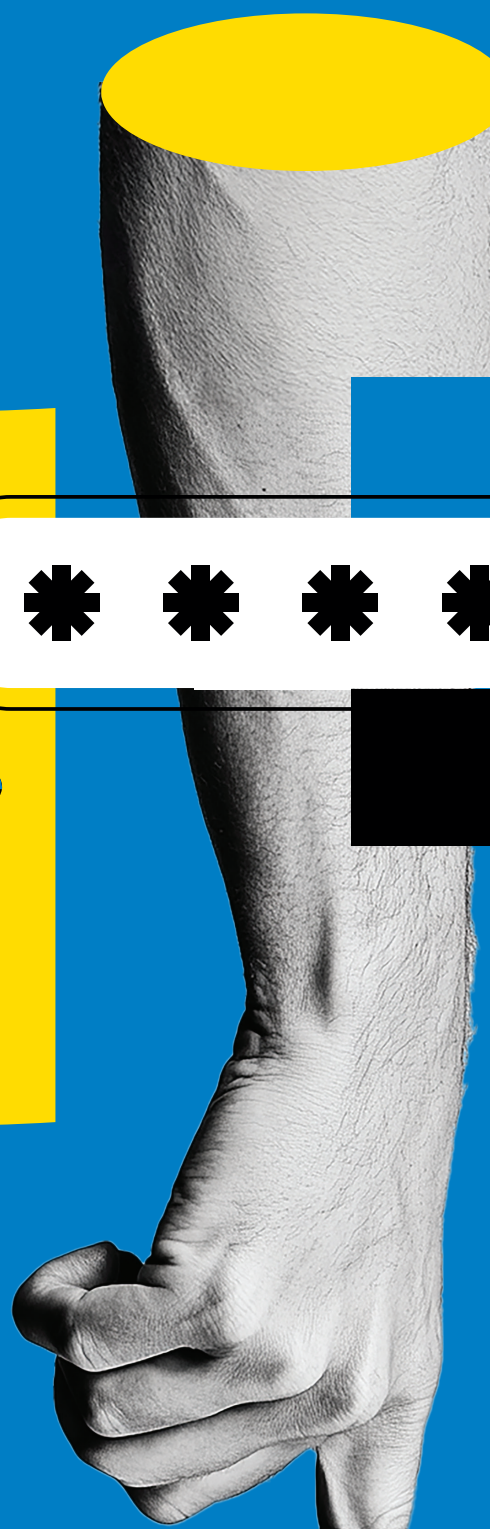
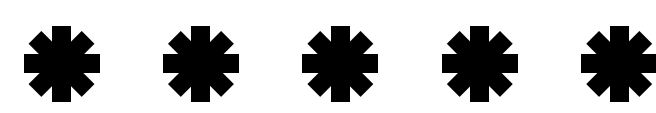
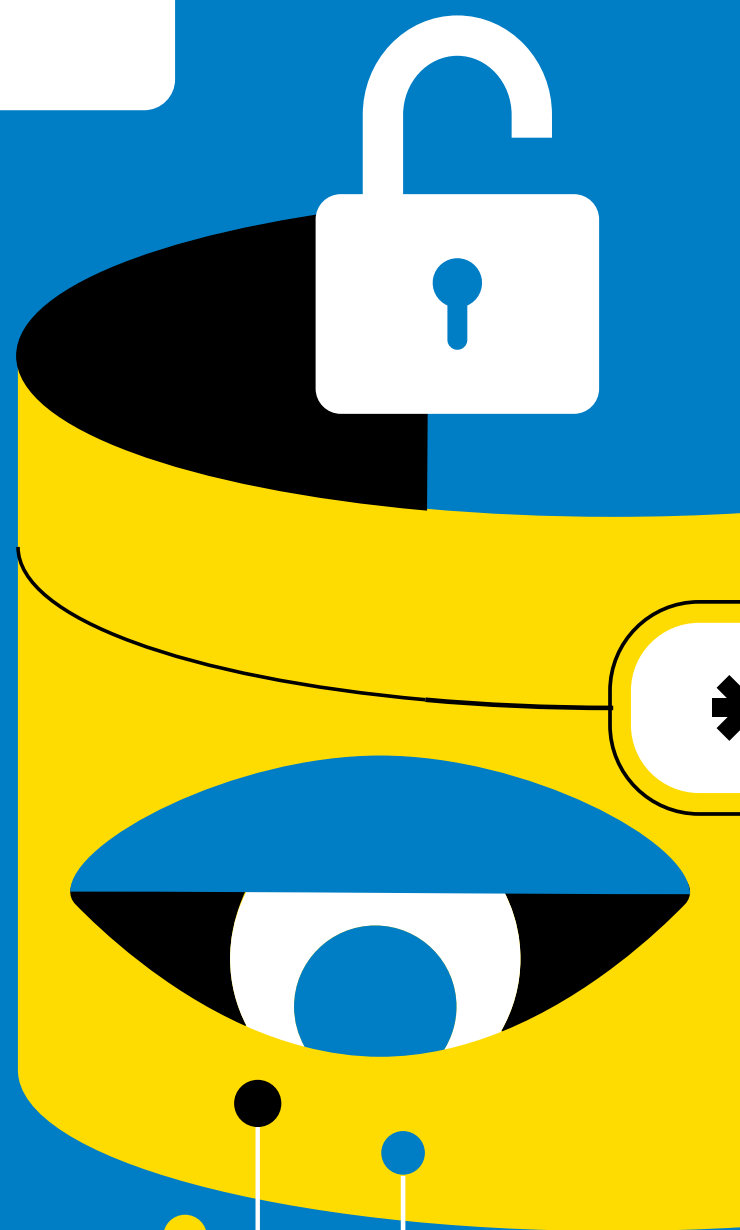
MALWARE

Installeer alleen legitieme en vertrouwde software, bij voorkeur via het officiële portaal van het bedrijf of rechtstreeks via de website van de leverancier.



GIJZEL-SOFTWARE

Hou je software en besturingssysteem goed up-to-date zodat kwetsbaarheden niet uitgebuit kunnen worden om gijzelsoftware te installeren.



ZWAKKE WACHTWOORDEN

Bescherm je account door een uniek en sterk wachtwoord te gebruiken, meerdere methoden voor multifactorauthenticatie in te stellen en wachtwoorden op te slaan in een persoonlijke wachtwoordmanager die beveiligd is met een lang en moeilijk te raden wachtwoord.



SOCIAL ENGINEERING

Verifieer verdachte e-mails altijd via een veilig tweede kanaal, zoals een telefoongesprek, om hun legitimiteit te bevestigen.



DATA LEKKEN

Om gegevens veilig te houden, bewaar je je data op de door het functiedomein ICT ondersteunde opslagplatformen en neem waar nodig bijkomende maatregelen, zoals encryptie van gevoelige data.

BLIJF EEN CYBER-DREIGING VOOR

Jij bent een belangrijke schakel in de veiligheidsketen!

WAT KAN JE DOEN?

MERK JE IETS VERDACHTS?

Breng de IT-helpdesk zo snel mogelijk op de hoogte via helpdesk.ugent.be/helpme

VERGROOT JE KENNIS!

Volg onze online IT-security training via helpdesk.ugent.be/security-training

KEN EN VOLG DE REGELS EN AFSPRAKEN

Lees de richtlijnen en het beleid voor veilig werken via helpdesk.ugent.be/security

