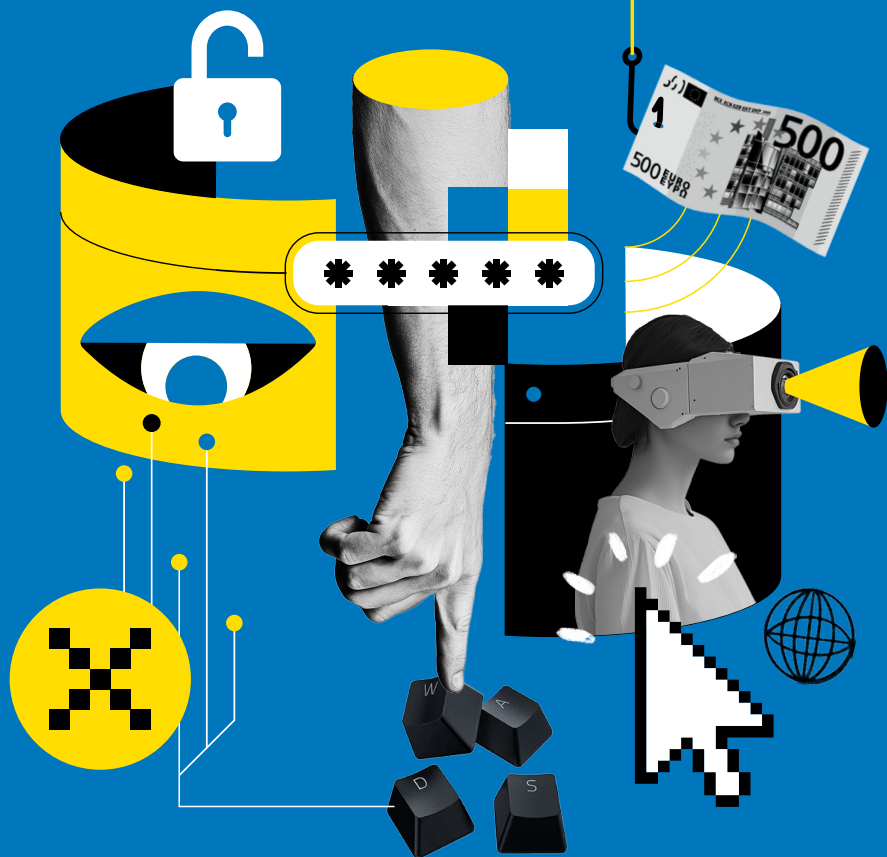




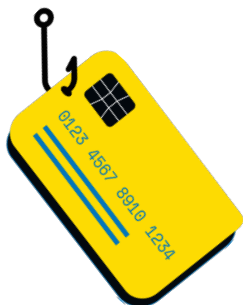
CYBERSECURITY

**Jij bent een belangrijke schakel
in de veiligheidsketen!**



**UNIVERSITEIT
GENT**

PHISHING



Bij phishing proberen cybercriminelen je te misleiden door zich in een e-mail voor te doen als een betrouwbare bron.

Als je in hun val trapt, dan kun je onbedoeld gevoelige informatie prijsgeven of je toestel infecteren met malware, wat kan leiden tot een datalek, identiteitsdiefstal, financieel verlies of erger.

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

Gijzelsoftware of ransomware vergrendelt bestanden of systemen en eist losgeld om weer toegang te krijgen, in het ergste geval op universiteitsbrede schaal.

Zo kunnen volledige netwerkschijven van onderzoeksgroepen vergrendeld worden omdat één enkele persoon ten prooi viel aan gijzelsoftware. **Hou je software en besturingssysteem daarom goed up-to-date** zodat kwetsbaarheden niet uitgebuit kunnen worden om gijzelsoftware te installeren.

GIJZEL-SOFTWARE



ZWAKKE WACHTWOORDEN

(EN WACHTWOORD HERGEBRUIK)

Zwakke wachtwoorden die eenvoudig te raden zijn of wachtwoorden die op verschillende plaatsen worden hergebruikt, vallen gemakkelijk ten prooi aan hackers.

Wanneer een aanval je wachtwoord bemachtigt, gaat die daar zeker mee aan de slag. **Gebruik voor je UGent-account dus altijd een uniek en sterk wachtwoord en stel meerdere methodes voor multifactor authenticatie in.** Gebruik een persoonlijke wachtwoord-kluus en vergrendel die met een lang en moeilijk te raden wachtwoord.



MALWARE



Malware is een verzamelnaam voor schadelijke software zoals virussen, spyware en trojans die je apparaten kunnen besmetten en gegevens kunnen stelen of vernietigen.

Malware kan je bestanden stelen of aanpassen, systemen vertragen, aanvallers laten meekijken met je activiteiten of in het ergste geval je hele toestel overnemen. Gekraakte software of downloads van niet officiële websites bevatten vaak malware. **Installeer daarom alleen legale, betrouwbare software**, bij voorkeur uit de company portal of rechtstreeks van de website van de leverancier.

Social engineering is een reeks oplichtings-technieken die inspelen op menselijke eigenschappen zoals nieuwsgierigheid, vertrouwen en onwetendheid, maar evengoed hebzucht en angst.

Daarmee worden slachtoffers gemanipuleerd om vertrouwelijke informatie vrij te geven of frauduleuze acties uit te voeren. Aanvallers kunnen technische beveiligingsmaatregelen omzeilen door personen te misleiden met bedrieglijke e-mails of telefoontjes. **Neem daarom contact op via een veilig tweede kanaal, bijvoorbeeld telefonisch, om na te gaan of een twijfelachtige e-mail legitiem is.**

SOCIAL ENGINEERING



DATA LEKKEN



Met een datalek wordt bedoeld dat persoonlijke of vertrouwelijke informatie zonder toestemming wordt geraadpleegd, gestolen of openbaar gemaakt.

Gelekte gegevens kunnen op allerlei manieren misbruikt worden of te gelde gemaakt. Een datalek kan leiden tot schade voor de UGent en voor individuele medewerkers en studenten. **Bewaar je data daarom op de door het functiedomein ICT ondersteunde opslagplatformen** en neem waar nodig bijkomende maatregelen, zoals encryptie van gevoelige data.

CYBERSECURITY: JIJ BENT EEN BELANGRIJKE SCHAKEL IN DE VEILIGHEIDSKETEN!

UGent neemt cyberveiligheid zeer ernstig. Met firewalls, antivirussoftware en monitoringsystemen zetten we een batterij aan hoogtechnologische maatregelen in om dagelijks de vele cyberdreigingen het hoofd te bieden. Maar technologische maatregelen alleen volstaan niet.

Jouw waakzaamheid en gezond verstand maken het verschil tussen een veilige omgeving en risico's op datalek of hacking. Daarom ben jij een cruciale schakel in onze verdedigingslinie.

WAT KAN JIJ DOEN?



MERK JE IETS VERDACHTS?

Merk je ongebruikelijke activiteit in een IT-toepassing of op een toestel? **Breng de IT-helpdesk zo snel mogelijk op de hoogte** via helpdesk.ugent.be/helpme. Snelle actie kan veel schade voorkomen!



VERGROOT JE KENNIS!

Cybercriminelen worden steeds slimmer, doe een tegenzet! **Volg onze online IT-security training** op helpdesk.ugent.be/security-training en leer hoe je bedreigingen kunt herkennen en voorkomen.



KEN DE REGELS EN AFSPRAKEN

Goed geïnformeerd zijn is de sleutel tot veilig werken. **Lees alle richtlijnen en afspraken** voor veilig werken op UGent via helpdesk.ugent.be/security

**SAMEN MAKEN WE UGENT VEILIGER.
BLIJF ALERT, WERK VEILIG!**