Cybercrime en gedigitaliseerde criminaliteit

Veiligheid voorop

« waakzaam en dienstbaar »

Cybercrime, do's en dont's

Steeds meer mensen worden het slachtoffer van cybercriminaliteit (hacking, ransomware, virussen etc.) of van gedigitaliseerde criminaliteit (zoals internetoplichting, afpersing via e-mail en phishing). Digitale veiligheid is helaas niet te garanderen. Je kunt wel maatregelen nemen om de kans om slachtoffer van cybercriminaliteit te worden zo klein mogelijk te maken.
We delen graag een aantal tips met je:

Beveiliging en updates

Gebruik sterke, unieke wachtwoorden, bijvoorbeeld lange zinnen, en verander je wachtwoord(en) geregeld.
Zorg dat je apparatuur goed beveiligd is en installeer updates zodra ze beschikbaar zijn.

Bijlages en links

Let op met het openen van bijlages van onbekende afzenders. Klik nooit zomaar op een link. Wanneer je met je muis over een link beweegt, zie je waar de URL naar toe leidt. Kijk goed wat er staat.

Gratis bestaat niet

Apps zijn nooit gratis. Je betaalt met geld of met gegevens over jezelf. Download je een gratis app, kijk dan goed wat deze app van je wil. Apps kunnen bijvoorbeeld toegang vragen tot je contacten, foto's en microfoon. Waarom zou je een navigatie-app toegang geven tot je camera? Lees goed wat een app met je gegevens doet en of jij dat acceptabel vindt voordat je toestemming geeft.

Meer informatie?
https://www.politie.nl/themas/cybercrime.html
https://veiliginternetten.nl

POL-268306-nl-NL-0419-1