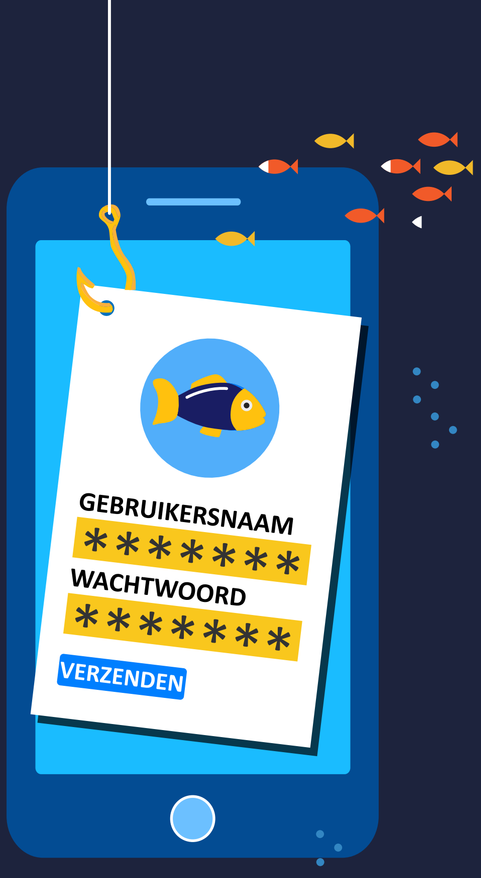
WEBGEBASEERDE RISICO'S

GOED OPLETTEN VOORDAT U KLIKT.

U kunt uw geld, persoonlijke gegevens en zelfs uw opgeslagen gegevens kwijtraken als het apparaat niet meer werkt.



WAT ZIJN DE RISICO'S?

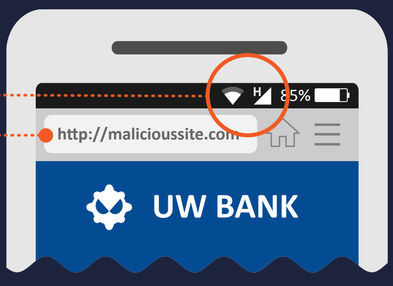
PHISHING-AANVALLEN: Tijdens een phishing-aanval proberen cybercriminelen achter de persoonlijke gegevens van internetgebruikers te komen door zich voor te doen als een betrouwbare partij. Zij zijn actief via e-mail, sms-berichten en sociale-mediaplatformen.

SURFEN OP INTERNET: Uw mobiele apparaat kan geïnfecteerd raken wanneer u een onveilige website bezoekt.

BESTANDEN DOWNLOADEN: E-mails kunnen kwaadwillende links of bijlagen bevatten.

WAAROM KAN HET GEBEUREN?

Mobiele apparaten zijn **ALTIJD VERBONDEN** met het internet.



Mobiele browsers geven de url's weer op een klein scherm. Op het **COMPACTE SCHERMFORMAAT** is het vaak moeilijk om te beoordelen of het domein betrouwbaar is.

Vanwege het persoonlijke karakter van een mobiele telefoon, zijn gebruikers geneigd om **ANDERE GEBRUIKERS AUTOMATISCH TE VERTROUWEN.**

WAT KUNT U DOEN?

Wees alert als een bedrijf u telefonisch of via sms vraagt om uw persoonlijke gegevens. Om te verifiëren of het bericht/telefoongesprek legitiem is, kunt u direct contact opnemen met het bedrijf door het officiële telefoonnummer te bellen.

Als u op internet surft met uw mobiele apparaat, let er dan op dat u websites bezoekt via HTTPS. U kunt dit altijd controleren door te kijken naar het begin van de url.

Klik nooit op een link of bijlage in een ongewenste e-mail of sms, maar verwijder de berichten direct.

Let ook goed op bij websites met grammaticale fouten, spelfouten en een lage resolutie.

Schakel automatische updates in. Installeer, indien mogelijk, een mobiele-beveiligingsapp die u op de hoogte stelt van verdachte activiteiten.

EUROPOL EC3 European Cybercrime Centre | POLITIE | ALERT online | Betaalvereniging Nederland

#MobileMalware