Enkele algemene tips:

- Als u het niet vertrouwt, ga dan nooit in op enige vraag tot betaling.
- Wat te mooi klinkt om waar te zijn, is het meestal ook.
- Een officiële instantie zal u nooit via e-mail, SMS, Whatsapp of telefoon vragen naar uw wachtwoord, bankgegevens of ander persoonlijke/gevoelige gegevens.
- Heeft u toch uw bankkaartgegevens doorgegeven, verwittig onmiddellijk cardstop. Contacteer hierna onmiddellijk uw bank.
- Criminelen maken websites tot in detail na. Men kan dit controleren in de koppeling van de website (www.voorbeeld.be). Als u twijfelt, stop dan onmiddellijk alle transacties.
- Beveilig uw accounts met sterke wachtwoorden en/of tweestapsverificatie.
- Installeer steeds een antivirussoftware op uw computer en hou deze up to date.
- Denkt u dat u gehackt bent, koppel het besmette systeem los van het internet.
- Deel geen intieme beelden van uzelf via internet en al zeker niet met mensen die u niet kent.

De aangifte:

Als u toch slachtoffer bent geworden van cybercrime, doet u best aangifte bij de politie. Verzamel hiervoor zoveel mogelijk informatie zoals:
- Bankafschriften
- E-mails
- Telefoonnummers/contactgegevens
- Namen van verdachte(n)
- Schermafdrukken van profielen/ gesprekken/ betalingen/ zoekertje...
- Websiteadressen
- ...

SLACHTOFFER? CONTACTEER ONS!

Hemelakkers 40
2930 Brasschaat

03 650 35 00

PZ.Brasschaat@police.belgium.eu

NUTTIGE LINKS:

- www.safeonweb.be
- www.polfed-fedpol.be
- www.clicksafe.be
- www.saferinternet.be
- www.veiligonline.be
- www.febelfin.be
- www.ccb.belgium.be
- www.besafe.be/nl/veiligheidsthemas
- https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides

VERDACHTE MAILS?

Stuur ze naar: verdacht@safeonweb.be

CARDSTOP:

Bel naar 070 344 344

MELDPUNT:

Surf naar https://meldpunt.belgie.be

Cybercrime

Wat is dat?

Lokale politie Brasschaat

WAT IS CYBERCRIME?

Cybercrime is een overkoepelende term voor misdrijven die niet kunnen gepleegd worden zonder tussenkomst of gebruik van smartphones, computers en/of netwerken.

Gelet het fenomeen de laatste jaren enorm in opmars is, werd cybercrime opgenomen als aandachtspunt in het huidige zonaal veiligheidsplan van 2020 – 2025 van politiezone Zwijndrecht.

DOEL:

In deze folder willen wij u op een duidelijke en leesbare manier bewust maken van de meest voorkomende fenomenen inzake cybercrime. Hierdoor is de kans groter dat u een fenomeen herkent wanneer u dreigt slachtoffer te worden zodat u op tijd kan ingrijpen.

We geven u ook enkele algemene tips mee waarmee u kan voorkomen dat u slachtoffer wordt van dergelijke misdrijven.

Tot slot leggen we uit wat u kan doen indien u toch slachtoffer geworden bent van cybercrime.

Phishing:

Phishing is een vorm van internetfraude waarbij u valse berichten ontvangt waarbij geprobeerd wordt om inloggegevens, creditcardinformatie, pincodes of andere persoonlijke gegevens te achterhalen.

Bv.: U ontvangt een SMS van 'uw bank' waarin wordt aangegeven dat u een nieuwe kaartlezer moet aanvragen. U wordt naar een valse website verwezen waar u uw gegevens en uw codes moet ingeven. Nadat u dit gedaan heeft, plundert men uw bankrekening.

Emotiefraude:

Emotiefraude is een vorm van internetfraude waarbij de verdachte zich voordoet als een iemand die u kent. Nadat ze vervolgens uw vertrouwen hebben gewonnen, vragen de criminelen om een betaling uit te voeren. Criminelen zoeken vaak op voorhand naar persoonlijke informatie via uw sociale media-kanalen.

bv.: U krijgt een bericht via Whatsapp van een onbekend nummer waarin 'uw zoon' aangeeft dat zijn GSM stuk is en dat dit zijn nieuw nummer is. Na een kort gesprek vraagt hij u enkele betalingen uit te voeren omdat hij 'problemen' heeft met zijn bank.

Oplichting met internet:

Oplichting met internet is een vorm van bedrog waarbij iemand u geld of goederen probeert afhandig te maken via misleiding op het web.

Bv.: U gaat in op een zoekertje op een tweedehandssite. U betaalt deze goederen maar krijgt deze vervolgens nooit toegestuurd. De 'verkoper' is plots ook niet meer bereikbaar.

Sextortion:

U werd overtuigd om intieme beelden van uzelf door te sturen en u wordt nu gedwongen om geld te betalen om verspreiding ervan te voorkomen of u ontvangt een e-mail waarin oplichters beweren dat ze intieme beelden van u bezitten en deze zullen verspreiden tenzij u geld betaalt.

Hacking:

Uw account werd gehackt waarbij er zonder uw medeweten berichten werden verstuurd naar uw contactpersonen of berichten of foto's op uw account werden geplaatst. Het doel kan het bekomen van financieel voordeel zijn, maar het kan ook een vorm van pesten of laster zijn.

Datasabotage:

U kreeg een melding van een virus op uw computer of uw computer werd geblokkeerd en u heeft geen toegang meer tot uw bestanden. Vervolgens vraagt men u om 'losgeld' zodat u opnieuw over de gegevens kan beschikken