

The logo for 'beringen' features a stylized lowercase 'b' with a yellow-green diagonal stroke on its left side and a teal circular element on its right side. The remaining letters 'eringen' are in a dark grey, sans-serif font.

The logo for 'beringen' features a stylized lowercase 'b' with a green-to-yellow gradient. The rest of the word 'beringen' is in a dark grey, sans-serif font.

Cyber veiligheid

Laat je niet b.dotten!

Door wie?

Dienst integrale veiligheid

- Opgericht in 2019
- Dienst
 - 1 manager integrale veiligheid
 - 1 noodplanningscoördinator
 - 1 deskundige integrale veiligheid
 - 7 Gemeenschapswachten/vaststeller
- Ikzelf
 - Niels Dirikx
 - Deskundige IV sinds september 2020
 - Coördinatie Gemeenschapswachten
 - Preventieve acties
 - Samenwerking andere diensten en organisaties



Acties cyberveiligheid

Samenwerkingen

Intern:

- Bibliotheek
- Communicatie
- Informatieveiligheidscel
- ICT

Extern:

- Politie
- Buurtwerking en dienstencentrum
- Digipunten

Acties cyberveiligheid

Aanpak

- Opmaak communicatie plan
 - Voorjaar 2022
 - Ism communicatieverantwoordelijk PZ
 - Overleg communicatiedienst
 - Planning
 - Timing
 - Overleg met BIB en digipunten
 - Spreiding communicatie over diverse mediakanalen in combinatie met infomomenten



Acties cyberveiligheid

Overzicht mediakanalen

- B-magazine
 - Juni
 - Oktober
- Sociale mediakanalen
 - Stad en PZ en BIB
 - Facebook
 - Instagram
- Persberichten
- Stadsapp
- Politiekrant
- Externe kanalen
 - UIT databank
 - Internetgazet kalender
 - HBVL evenementen kalender



B-magazine



Oplichting en cybercriminaliteit

Fraude en oplichting doen zich vaak voor via internet of sociale media. Dank aan fraude bij online kopen en verkopen via een valse advertentie of de vraag om een voorschot te betalen. Ook vriendschapsfraude, alle vormen van phishing (via e-mail of WhatsApp) en valse profielen op sociale media zijn vormen van cybercriminaliteit. Blijf steeds op je hoede. Komt een bericht uit onverwachte hoek? Word je onder tijdsdruk gezet? Worden er vertrouwelijke gegevens gevraagd? Merk je taalfouten op? Dit zijn allemaal zaken waarvan jouw alarmbelletjes moeten afgaan, want dan is de kans op oplichting groot.

ONTVANG JE FRAUDULEUZE MAILS OF BERICHTEN?

- ✓ Klik niet op een link in een verdacht bericht.
- ✓ Heb je toch al geklikt, vul de velden dan niet verder in en breek elke interactie af. Contacteer ofwel je bank die eventuele maatregelen kan nemen of Card Stop om je kaart te blokkeren. Dit kan dag en nacht op T 078 170 170.
- ✓ Valse e-mails en berichten, of een screenshot hiervan, kan je doorsturen naar verdscht@safeonweb.be. De inhoud wordt automatisch verwerkt.

HOE?

- ✓ Gaat het om feiten die **niet langer dan 2 werkdagen geleden** financieel verlies **meer dan 500 euro**? Neem dan onmiddellijk contact op met de lokale politie Beringen/Ham/Tessenderlo. Binnen de kantooruren kan je steeds terecht op T 011 27 95 79.

Buiten de kantooruren neem je contact op via T 101. Dit alles met het oog op het noteren van een aangifte en het proberen te recupereren van jouw financieel verlies.

- ✓ Laat dit je uiteraard niet tegenhouden om bij een lager bedrag toch aangifte te doen. Als je twijfelt neem je contact op met de diensten van de politie via T 011 27 95 79.

MEEBRENGEN?

Om de aangifte vlot te kunnen laten verlopen, raden wij jou aan om volgende zaken mee te brengen:

- ✓ je identiteitskaart;
- ✓ de (ingevulde) vragenlijst die je kan vinden op de website van politie Beringen/Ham/Tessenderlo;
- ✓ een gedetailleerd rekeningoverzicht indien er geld van je rekening is;
- ✓ afgeprinte bewijsstukken van gesprekken met verdachten;
- ✓ de login-gegevens van jouw account waarop fraude is gepleegd.

INFO

Tijd kost geld. Doe je aangifte zo snel mogelijk bij de lokale politie Beringen/Ham/Tessenderlo.

Politie Beringen/Ham/Tessenderlo
T 011 27 95 79



Laat je niet b.dotten

WAT IS CYBERCRIMINALITEIT?

Cybercriminaliteit is criminele activiteit die zich richt op een computer, smartphone of je thuisnetwerk. Hiervoor wordt bijvoorbeeld gebruik gemaakt van e-mail, WhatsApp, sms of sociale media. Fraude en oplichting doen zich vaak voor via internet of sociale media. Klinkt iets te mooi om waar te zijn? Dan zouden er alarmbelletjes moeten afgaan, want de kans op oplichting immers groot.

De meeste, maar niet alle, cybercriminaliteit wordt gepleegd door cybercriminelen of hackers om geld te verdienen. Cybercriminaliteit wordt uitgevoerd door individuen of organisaties.

Sommige cybercriminelen zijn georganiseerd, maken gebruik van geavanceerde technieken en zijn hoog opgeleid. Anderen zijn onervaren hackers.

Cybercriminaliteit is vrijwel altijd gericht op geld. Andere redenen zijn politiek van aard of hebben een persoonlijke achtergrond.

INFO

'De criminele toekomst: Cybercrime' door Jos Delarbre

Maak je je zorgen over cybercriminaliteit? Als je begrijpt wat cybercriminaliteit is, wat de verschillende types zijn en hoe je jezelf er tegen kunt beschermen, slaap je vast beter.

Deze infoessie gaat dieper in op cybercriminaliteit, zodat je precies weet

tegen welke bedreigingen je jezelf moet beschermen om veilig online te zijn. We bespreken:

- ✓ Wat is cybercriminaliteit?
- ✓ Verschillende types van cybercriminaliteit.
- ✓ Wat wordt beschouwd als cybercriminaliteit, met voorbeelden.
- ✓ Bescherming tegen cybercriminaliteit.

Na de infoessie zal een inspecteur van de politiezone BHT een toelichting geven over wat je moet doen indien je slachtoffer werd van cybercrime.

di 25 oktober om 19.00 uur in het Lokaal Buurthuis Steenveld, Nachtegaalstraat 83, 3582 Beringen.



www.beringen.be

Wil je een aangifte of melding doen bij de politie? Dit kan via www.politie-bht.be/nl/aangifte-of-melding-doen

Ben je slachtoffer van oplichting of cybercriminaliteit? Aangifte doen kan via www.politie-bht.be/nl/icheel/143/oplichting-en-cybercriminaliteit

Samen één voor een veilige buurt

Woninginbraken blijven overal in onze provincie een maatschappelijke plaag, ook binnen onze politiezone. Het buurtpreventienetwerk wil dat buurtbewoners elkaar attent maken op zaken die spelen in de buurt. Zo kunnen ze samen een oogje in het zeil houden en sneller verdachte situaties melden bij de politie. Deze werkwijze verhoogt de sociale controle en heeft als doel inbraken zoveel mogelijk te voorkomen.

OP ZOEK NAAR NIEUWE LEDEN

Het buurtpreventienetwerk is continu op zoek naar nieuwe leden en wil zoveel mogelijk burgers warm maken om het initiatief te vervoegen om samen 'gewapend' de donkere wintermaanden in te gaan. **Immers, hoe meer sociale controle, hoe veiliger de buurt of ... hoe meer buurten veiliger!**

INFO ✓ Om lid te worden van onze buurtpreventiegroep surf je best naar de website van de lokale politie Beringen/Ham/Tessenderlo: www.politie-bht.be. Je vraagt het lidmaatschap dan online aan en het is volledig gratis.



Filmpjes sociale media



Acties cyberveiligheid

Overzicht acties digitale maand cyberveiligheid

Laat je niet b.dotten

- Infosessie digitaal bankieren door Febilfin
 - 1x in bibliotheek
 - 1x in dienstencentrum
- Infosessie cyberveiligheid door Jos Delarbre en PZ
 - Locatie buurthuis Steenveld
- Digibabbels in de digipunten
 - 1x per week, steeds ander thema

WEEK 1 vanaf maandag 3 oktober in alle Beringse digipunten
Safeonweb app/website - online oplichting herkennen, voorkomen en melden

WEEK 2 vanaf maandag 12 oktober in alle Beringse digipunten
Payconiq App – veilig digitaal betalen

WEEK 3 vanaf maandag 19 oktober in alle Beringse digipunten
Veilige wachtwoorden – veilig online

WEEK 4 vanaf maandag 26 oktober in alle Beringse digipunten
Vingerafdruk, code, gezichtsherkenning – beveiliging van je smartphone



Acties cyberveiligheid

Bibliotheek

Vast aanbod doorheen het jaar in de BIB

- Collectie boeken veilig online
 - Aanbod beschikbaar via website
 - Themastand in de BIB
- Edubox
 - Lespakket VRT
 - Beschikbaar in de BIB
- Info fiches via digibabbels
- Budget werking mediawijsheid
 - Lezingen, infosessies, workshops, ...
 - Afgestemd op behoefte
- 2 media coachen
 - Opleiding mediawijs en IMEC



Acties cyberveiligheid

Intern binnen Stad Beringen

- Oprichten informatieveiligheidscel
- Pentest
 - Fysieke controle ivm toegang
 - Digitaal
 - Ethical hacker
 - Software, phishing, ...
- Opmaak business continuityplan
- Informatie voor werknemers
 - Intranet
 - Digitale schermen



