

# WEES MALWARE BEWUST

Malware is kwaadaardige software die gebruikt wordt om computersystemen te verstoren, gevoelige informatie te verzamelen of toegang te krijgen tot private computersystemen met als doel het schenden van uw privacy. Voorbeelden van Malware : virussen, wormen, trojans, spyware, ransomware,....

## EERST KIJKEN DAN PAS KLIKKEN

1

Beweeg de muis boven de hyperlink in de e-mail. Kijk of de link klopt en of het veilig is (HTTPS). Onthoudt dat banken e.d. nooit een link sturen in hun email om in te loggen. Bij twijfel bellen. Reageer niet per e-mail.

## REAGEER NIET OP SPAM

2

Gewoon negeren, niet reageren en zeker niet klikken.



## KLIK NIET OP ADVERTENTIES

6

Sommige advertenties kunnen ook malware installeren. Klik daarom nooit op advertenties.

## GEEF NOOIT WACHTWOORDEN

5

Word je gebeld door iemand die je niet kent? Geef NOOIT je wachtwoord. Het maakt niet uit van welk bedrijf ze bellen of voor wie het is.

## VREEMDE POP-UPS

10

## BEL DIRECT IT-SUPPORT

Krijg je opeens reclame te zien of geeft je computer vreemde meldingen? Stop direct de internetverbinding (haal je kabel uit het apparaat of zet je WiFi uit). Zet apparaat niet uit anders kunnen digitale sporen verloren gaan.

## KLOPT DE BIJLAGE

3

Open nooit bijlagen verzonden per e-mail door onbekenden mensen. Kijk bij bekende mensen of de tekst in de e-mail wel klopt. Bij twijfel, bel de persoon eerst even op.

## GEBRUIK BEDRIJFS- APPARATUUR NIET PRIVE

7

Bezoek geen websites en installeer geen software, als het niet nodig is voor het bedrijf

## USB STICK GEVONDEN OF GEKREGEN

11

USB sticks worden door hackers expres achtergelaten of weggegeven op bv. beurzen. Gooi gevonden USB-sticks altijd weg en wees voorzichtig met verkregen USB-sticks.

## GEBRUIK ALTIJD ANTIVIRUS- SOFTWARE

12

Zorg dat je goede antivirussoftware gebruikt en deze automatisch laat updaten.

## KLOPT DE WEBSITE

4

Bekende websites worden door hackers nagebouwd om uw inloggegevens te stelen. Kijk of de link veilig is (HTTPS) en of de URL klopt.

## GRATIS WIFI IS GEVAARLIJK

8

Log niet in op gratis, onbeveiligde WiFi netwerken. Je PC of netwerk is zo gehackt.



## 123AUTOMATISERING voorsprong door service

## BEWAAR JE BESTANDEN

9

## OP DE JUISTE PLEK

Bij ransomware worden je bestanden geblokkeerd. Bewaar daarom je bestanden op de aangegeven plek. Dan kan de IT afdeling er een back-up van maken.

## GEBRUIK ALTIJD VERSCHILLENDE WACHTWOORDEN

13

Gebruik verschillende wachtwoorden voor meerdere accounts en verander ze minimaal ieder jaar. Zorg ook voor sterke wachtwoorden. Die zijn moeilijk te raden en te kraken.

## GEBRUIK EEN RECENT BESTURINGSSYSTEEM

14

Zorg dat je een recent besturingssysteem gebruikt en deze automatisch of regelmatig laat updaten.

## WEES BEWUST OP INTERNET GEEF INTERNETCRIMINELEN GEEN KANS

## DOWNLOAD GEEN BESTANDEN

Pas op met het zomaar downloaden van bestanden op het internet.

↓ 15