DELL Technologies

Cheat-blad cyberveiligheid

In onze groeiende virtuele wereld, groeit cybercriminaliteit, niet geheel verrassend, in een alarmerend tempo. **Cybercriminaliteit heeft in 2021 ongeveer $ 6 biljoen gegenereerd** waarmee het de derde grootste economie ter wereld is, na de VS en China![1] Aanvallers worden met de dag slimmer en geraffineerder, maar u kunt eenvoudig veilig online zijn als u op de hoogte bent van de nieuwste bedreigingen en beschermende maatregelen neemt. **Hier zijn enkele voorbeelden van bedreigingen die cyberveiligheidsexperts van Dell proberen te voorkomen en tips over hoe u uw werkplek en apparaten thuis veilig kunt houden.**

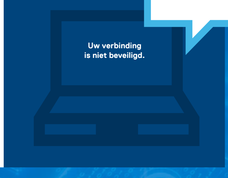
Drive-by aanvallen

Vijandige groepen krijgen toegang tot uw systeem wanneer u een onbeveiligde of gecompromitteerde website bezoekt.

Hoe u dit kunt herkennen:

Nieuwe bestanden of netwerkverbindingen op uw systeem die u niet hebt toegevoegd

Ongevraagde verzoeken om configuratiegegevens



TIP: Houd browsers en plug-ins up-to-date

Onveilige hardware

TIP: Doe uw aankopen via geautoriseerde verkopers

Bedreigende partijen integreren kwetsbaarheden rechtstreeks in hardware en accessoires.

Hoe u dit kunt herkennen:

Deals die te mooi zijn om waar te zijn

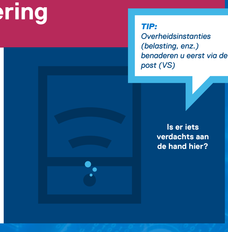
Social-engineering

Een scammer manipuleert mensen door zich voor te doen als een rechtspersoon of ander gezaghebbend orgaan om gevoelige **persoonlijke of financiële gegevens** te stelen (ook bekend als 'phishing'). De schadelijke code wordt via koppelingen of bijlagen bij e-mails, chatberichten of sms-berichten verstuurd.

Hoe u dit kunt herkennen:

Ongevraagde e-mails of sms-berichten waarin om persoonlijke gegevens wordt gevraagd met aanwijzingen om koppelingen en bijlagen te openen

Vreemd e-mailadres van de afzender, vreemde frasering of foute spelling



TIP: Overheidsinstanties (belasting, enz.) benaderen u eerst via de post (VS)

Malware-aanval via USB

TIP: Pas op voor onbekende USB-sticks, zelfs als ze erkomstig zijn van vrienden

Een crimineel gebruikt verwijderbare storageapparaten, zoals USB-sticks, draagbare harde schijven, smartphones, muziekspelers, SD-kaarten en optische media (cd's dvd's, BluRay) om een computer of netwerk te infecteren.

Hoe u dit kunt herkennen:

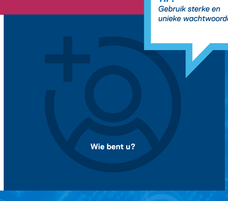
Onverwachte toegang tot bestanden of nieuw aangemaakte bestanden op het apparaat

Vertrouwde relatie

Een hacker breekt in bij een vertrouwde derde partij, zoals een dokterspraktijk, en gebruikt hun goede reputatie om patiënten uit te buiten.

Hoe u dit kunt herkennen:

Ongebruikelijk inloggedrag



TIP: Gebruik sterke en unieke wachtwoorden

Hoe u cyberveilig blijft:

DOEN

Gebruik meervoudige verificatie en sterke, unieke wachtwoorden voor al uw accounts.

Elk apparaat dat met het internet is verbonden, kan worden aangevallen. Houd software up-to-date.

Wees alert en kritisch. Leer tactieken van scammers herkennen.

Praat erover. Rapporteer aanvallen op IT en houd collega's, familie en vrienden op de hoogte.

NIET DOEN

Word niet lui. Volg alle beveiligingsprotocollen consistent op.

Klik nooit op koppelingen die in onverwachte e-mails of chatberichten staan.

Negeer de waarschuwingen van de browser niet, bijv. "Uw verbinding is niet beveiligd" of "Uw verbinding is niet privé".

TIP: Ga voor meer informatie naar: Dell.com/Endpoint-Security

DELL Technologies

[1] Bedrijven voor cyberbeveiliging: Almanak cyberveiligheid 2022; 100 feiten, grafieken, voorspellingen en statistieken

Copyright © 2022 Dell Inc. of haar dochterondernemingen. Alle rechten voorbehouden. Dell Technologies, Dell, EMC, Dell EMC en andere handelsmerken zijn handelsmerken van Dell Inc. of haar dochterondernemingen. Andere handelsmerken zijn mogelijk handelsmerken van hun respectieve eigenaren. Deze casestudy is alleen voor informatiedoeleinden. Dell is van mening dat de informatie in deze casestudy correct is op de publicatiedatum, september 2022. De informatie kan zonder voorafgaande kennisgeving worden gewijzigd. Dell geeft geen expliciete of impliciete garanties in deze casestudy.