



SEIZOENSTIP



Cyberveiligheid

In deze rubriek belichten we doorgaans een 'good practice' die andere uitbaters kan inspireren. Deze keer zoomen we in op een thema dat elke uitbater aanbelangt: cyberveiligheid. Wat betekent het om gehackt te worden? Welke risico's zijn er vandaag? En vooral: wat kan je zelf doen om je gegevens digitaal veilig te houden?

Waarom cyberveiligheid belangrijk is

Veel jeugdverblijven werken vandaag bijna uitsluitend digitaal. Je beheert reservaties via mail of een online systeem, wisselt documenten uit via mail, bewaart gegevens in de cloud, verwerkt betalingen digitaal ... Die digitalisering brengt nieuwe risico's met zich mee. Je bewaart veel informatie van groepen, vrijwilligers en medewerkers. Denk aan contact- en identiteitsgegevens, facturatiegegevens, deelnemerslijsten en soms zelfs medische informatie. Als je persoonsgegevens bewaart, ben je volgens de privacywetgeving verantwoordelijk voor een veilige opslag en een beperkt gebruik ervan.

Veel mensen denken dat cybercriminaliteit vooral een probleem is voor grote bedrijven. Toch zijn ook kleine organisaties en particulieren vaak een doelwit. Cybercriminelen weten dat die vaak minder tijd, kennis en middelen hebben om hun digitale omgeving op te volgen. Gehackt worden heeft dan ook niets te maken

met dom zijn. Cybercriminelen spelen vooral in op tijdsdruk, vertrouwen en routine. Eén onoplettend moment kan al genoeg zijn. Door te weten waar de risico's zitten, kan je al veel problemen voorkomen.

Wat is hacking?

Gehackt worden betekent dat iemand zonder toestemming binnenkomt in je digitale omgeving. Dat kan gaan om je computer, cloudopslagsysteem, mailbox, website, reservatiesysteem of online boekhouding. Soms willen hackers persoonsgegevens bekijken of stelen. Soms proberen ze geld af te troggelen door facturen aan te passen of geldstromen om te leiden. In andere gevallen sturen ze berichten uit in naam van jouw organisatie of blokkeren ze je computer of server. Je krijgt dan een melding met de vraag om geld te betalen om alles terug vrij te krijgen.

Als gegevens verloren gaan of misbruikt worden, kunnen de gevolgen dus groot zijn. Je verliest toegang tot belangrijke documenten, reservatiegegevens raken onbeschikbaar, persoonsgegevens lekken uit, betalingen worden omgeleid en tot slot kunnen klanten en partners hun vertrouwen verliezen.

Hackers gebruiken verschillende methodes om binnen te raken. Sommigen maken misbruik van technische kwetsbaarheden in

software of online toepassingen, maar veel aanvallen slagen door menselijke fouten. E-mail is daarbij vaak het belangrijkste doelwit. Want wie toegang krijgt tot een mailbox, kan berichten versturen in jouw naam, facturen onderscheppen, wachtwoorden resetten en toegang proberen te krijgen tot andere accounts. De twee meest voorkomende risico's zijn een zwakke toegangsbeveiliging en phishing.

Toegangsbeveiliging

Accounts met zwakke wachtwoorden of onvoldoende toegangsbeheer zijn een makkelijk doelwit voor cybercriminelen. In jeugdverblijven werken vaak verschillende beroepskrachten, vrijwilligers of tijdelijke krachten samen. Daardoor worden wachtwoorden soms gedeeld of worden privé- en werkaccounts door elkaar gebruikt. Dat lijkt soms handig, maar verhoogt het risico op fouten en misbruik. Als meerdere mensen hetzelfde account gebruiken, is het bovendien moeilijk om te achterhalen wie welke actie uitvoerde. Met een paar eenvoudige maatregelen kan je veel risico's beperken.

1. Maak duidelijke afspraken

Cyberveiligheid is een gedeelde verantwoordelijkheid. Duidelijke afspraken helpen om risico's te beperken. Spreek af wie toegang heeft tot welke systemen, wie facturen controleert, wie je contacteert bij twijfel, hoe nieuwe medewerkers toegang krijgen en wanneer toegangen worden verwijderd. Moedig ook aan om vragen te stellen bij twijfel. Niet iedereen heeft evenveel ervaring met digitale toestellen, apps of online diensten.

2. Ga zorgvuldig om met persoonsgegevens

Veel jeugdverblijven bewaren documenten in gedeelde mappen of sturen ze via mail. Werk daarom best met beveiligde cloudopslag. Bewaar documenten met persoonsgegevens niet langer dan nodig (deelnemerslijsten moet je bijvoorbeeld 7 jaar bijhouden en boekhoudkundige documenten 10 jaar). En vermijd het rondsturen van documenten met veel persoonlijke gegevens.

3. Gebruik sterke wachtwoorden

Een sterk wachtwoord is nog altijd één van de beste vormen van beveiliging. Wachtwoorden zoals de naam van je uitbating zijn snel te raden. Als iemand eenmaal binnen is, kan die vaak ook andere accounts overnemen. Enkele tips:

- gebruik lange wachtwoorden of wachtwoordzinnen met minstens 15 karakters;
- gebruik cijfers, hoofdletters en symbolen;
- gebruik voor elk account een ander wachtwoord;
- deel wachtwoorden niet (of toch zo weinig mogelijk) met anderen;
- gebruik eventueel een wachtwoordkluis (wachtwoordmanager). Dit is een digitale omgeving waarin je al je inloggegevens en wachtwoorden veilig bewaart. Microsoft en Google hebben beiden een gratis Password Manager. Betalende oplossingen zoals bijv. 1Password, Nordpass en Bitwarden kunnen interessant zijn als je wachtwoorden veilig wil delen en beheren binnen een team;
- werk waar mogelijk met tweestapsverificatie (2FA), waarbij je na je wachtwoord een tweede bewijs van je identiteit moet geven. Zowel Microsoft als Google heeft een gratis authenticator voor 2FA.

4. Hou je website en software up-to-date

Verouderde software vormt een risico. Computers, reservatiesystemen, websites en andere digitale toepassingen krijgen regelmatig beveiligingsupdates. Als je die updates niet uitvoert, blijven gekende zwakke plekken openstaan. Controleer dus regelmatig of je website en reservatiesysteem up-to-date zijn.

5. Maak back-ups

Als een computer crasht of bestanden gegijzeld worden, kan een back-up veel problemen voorkomen. Maak regelmatig een reservekopie van belangrijke documenten en reservatiegegevens. Bewaar die op een andere locatie of in een betrouwbare cloud-omgeving. Controleer af en toe of je de back-up effectief kan terugzetten.

6. Beveilig je wifi-netwerk

Als je wifi aanbiedt aan groepen, zorg je er best voor dat je wifi-netwerk veilig is. Gebruik bij voorkeur een apart gastnetwerk voor bezoekers en scheid dit van toestellen en systemen die je zelf gebruikt. Zorg daarnaast voor een sterk wifiwachtwoord en werk je router en netwerkkapparatuur regelmatig bij. Verouderde of slecht beveiligde netwerkkapparatuur vormt een groter risico op misbruik.

De grootste dreiging van vandaag: phishing

Phishing is vandaag de meest voorkomende vorm van cybercriminaliteit. In 2025 werden zo'n 10 miljoen phishingpogingen gemeld via Safeonweb. Cybercriminelen gebruiken daarbij kanalen die je elke dag gebruikt, zoals e-mail, sms, WhatsApp of zelfs QR-codes die betrouwbaar lijken. De afzender doet zich bijvoorbeeld voor als een vertrouwde leverancier, bank, overheidsdienst of partnerorganisatie. Ze vragen je om op een link te klikken, een bijlage te openen of gegevens door te geven. Zo kunnen ze toegang krijgen tot je accounts, persoonsgegevens of financiële gegevens.

Phishing wordt steeds geloofwaardiger

Phishingberichten zijn vandaag moeilijker te herkennen. Dankzij artificiële intelligentie zijn ze beter geschreven en vaker afgestemd op jouw organisatie of situatie.



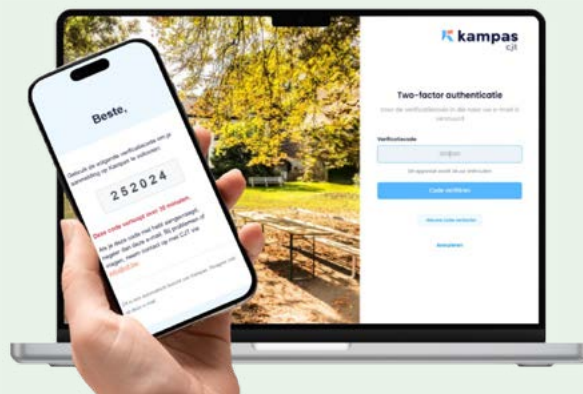
Gebruikersgegevens lekken regelmatig uit via datalekken bij bijvoorbeeld webshops, afsprakenplatformen of sociale media en worden verkocht op het 'darkweb'. Je kan op websites zoals Haveibeenpwned of Firefox Monitor nakijken of jouw gegevens gelekt zijn."

Uit de praktijk: kampas.be

Cyberveiligheid is ook voor Kampas een dagelijkse zorg. Het platform verwerkt persoonsgegevens en ondersteunt betalingen via de online boekingsmodule. Daarom werken we voortdurend aan een veilige en betrouwbare werking.

In samenspraak met de IT-partner houdt CJT de technische systemen in de eerste plaats up-to-date. Bovendien werden sinds de lancering enkele belangrijke stappen gezet om de beveiliging te verbeteren. Zo voerden we tweestapsverificatie in. Uitbaters kunnen ook voor elke gebruiker een apart account aanmaken, zodat ze geen wachtwoorden hoeven te delen. Daarnaast liet CJT kampas.be recent nog controleren door een ethische hacker. Dat is een beveiligingsexpert die met toestemming probeert zwakke plekken in een digitaal systeem op te sporen, zodat die kunnen worden opgelost vóór kwaadwillige hackers er misbruik van maken. Die controle leverde een positief rapport op, met enkele aandachtspunten die onze IT-partner meteen heeft aangepakt.

Een garantie van 100% bestaat uiteraard nooit. Daarom monitort onze IT-partner verdachte activiteiten op het platform, zodat die snel kunnen worden opgespoord en er tijdig kan worden ingegrepen.



Ook Kampas werkt al enige tijd met een tweestapsverificatie.

Ook factuurfraude komt vaker voor. Cybercriminelen onderscheppen facturen en passen het rekeningnummer aan. De factuur lijkt correct, maar het geld belandt op de rekening van een oplichter.

Zo herken je phishing

1. Klik nooit meteen. Krijg je een onverwachte mail of bericht met een link, een bijlage of een dringende boodschap ... Klik dan niet meteen. Hackers rekenen erop dat je snel reageert. Twijfelen is dus goed. Controleer eerst via een andere weg of de vraag klopt.
2. Controleer wie de mail stuurde. Kijk goed naar het emailadres van de afzender. Komt de naam bekend voor, maar klopt het adres niet helemaal? Zie je vreemde letters of extra cijfers? Dan is de mail waarschijnlijk vals. E-mails van CJT en Kampas worden bijvoorbeeld altijd verstuurd vanuit een adres dat eindigt op cjt.be en kampas.be.
3. Geloof geen tijdsdruk of dreiging. Phishingmails zetten je vaak onder druk, zoals: "Je account wordt vandaag afgesloten", "Betaal binnen 24 uur" of "Er is een probleem met je betaling". Wees dan extra alert.
4. Geef nooit gegevens door via email of telefoon, zoals wachtwoorden, codes, bankgegevens of identiteitsgegevens. Een bank, overheid of leverancier vraagt dit niet.

5. Open geen bijlage als je twijfelt. Zeker geen bijlagen met .zip, .exe of onverwachte facturen of scans. Eén klik kan al genoeg zijn om malware te installeren op je apparaat, dat is schadelijke software die gegevens kan stelen, systemen kan verstoren of bestanden kan versleutelen. Een bekende vorm hiervan is ransomware of gijzelsoftware, waarbij cybercriminelen je bestanden blokkeren en geld vragen om ze opnieuw vrij te geven.
6. Verwijder de mail of meld ze als spam of phishing in je mailprogramma. Gebruik je een gedeelde mailbox? Verwittig ook collega's of vrijwilligers, zodat niemand anders erop klikt. Als je zeker bent dat het om phishing gaat, kan je de mail rapporteren via safeonweb.be/nl/meld-incident.

Toch een hack of datalek ...

Merk je vreemde activiteiten op? Of heb je per ongeluk op een verdachte link geklikt, een bijlage geopend of gegevens doorgegeven? Handel dan meteen. Verander je wachtwoord en gebruik dat wachtwoord nergens anders meer. Meld het incident aan de persoon die IT opvolgt binnen je organisatie en ga na welke gegevens mogelijk getroffen zijn. Hoe sneller je reageert, hoe kleiner de kans op schade.

Denk je dat persoonsgegevens van klanten, vrijwilligers of medewerkers gelekt zijn? In sommige gevallen moet je een

datalek melden aan de Gegevensbeschermingsautoriteit. Neem contact op met je IT-partner, softwareleverancier of een andere deskundige die je kan helpen de impact in te schatten en de juiste stappen te zetten.

Kleine gewoontes die veel verschil maken

Je hoeft geen IT-expert te zijn. Met een paar eenvoudige gewoontes, duidelijke afspraken en een gezonde dosis alertheid verklein je het risico op problemen aanzienlijk. Zo bescherm je niet alleen je organisatie, maar ook je gasten, vrijwilligers en medewerkers:

- twijfel is een goeie reflex;
- vergrendel je computer wanneer je weggaat;
- gebruik geen openbare wifi voor administratie;
- installeer updates op tijd;
- maak regelmatig back-ups;
- gebruik sterke wachtwoorden;
- maak duidelijke afspraken binnen je team.



Meer tips en actuele waarschuwingen vind je op www.safeonweb.be.