techsoup GLOBAL

12 TIPS OM VEILIGER ONLINE TE ZIJN

Deze Gids voor Veiliger Internet is bedoeld voor non-profitorganisaties, goede doelen en NGO's.

U bent afhankelijk van de goodwill van uw donateurs, leden en achterban voor ondersteuning. Daarom is het beschermen van uw gegevens en infrastructuur erg belangrijk. Deze gids is bedoeld om u te helpen de informatie veilig te houden.

Onze 12 tips beslaan vier hoofdgebieden:

Op kantoor

Er zijn enkele fundamentele zaken waar u en uw medewerkers aan moeten denken tijdens het werken op kantoor. Leer ze voordat het te laat is.

Maak veilig gebruik van sociale media

Sites van sociale media behoren tot de meest bezochte sites. Houd rekening met zaken die u wel en juist niet moet doen als u ze gebruikt, zowel zakelijk als privé.

Buiten het kantoor

De meeste medewerkers gebruiken verschillende apparaten (zoals laptops, mobiele telefoons en tablets) en gebruiken die in openbare ruimtes. Pas deze nuttige tips toe als u buiten uw kantoor bent.

Maak veilig gebruik van de cloud

Online toepassingen slaan uw gegevens op internet op. Deze tips helpen ervoor te zorgen dat uw gegevens veilig en ongeschonden blijven.

techsoup GLOBAL

1 Maak het hackers moeilijker

Wees slim met wachtwoorden. Na de fysieke beveiliging van uw kantoor zijn wachtwoorden de op één na belangrijkste zaak. Gebruik sterke wachtwoorden met een combinatie van hoofd- en kleine letters, cijfers en speciale tekens. Dit helpt u te beschermen tegen hackers die willekeurig en systematisch wachtwoorden proberen te raden op basis van veelgebruikte woorden. En verder:

- ◯ Gebruik verschillende wachtwoorden voor verschillende sites. Gebruik speciale software voor het beheren van wachtwoorden om u te helpen ze te onthouden.
- ◯ Om het ongeautoriseerd terugvinden van wachtwoorden met behulp van algemeen bekende informatie (zoals uw geboortedatum, het model van uw eerste auto of de naam van uw huisdier) tegen te gaan, kunt u overwegen gerelateerde maar onzinnige antwoorden te geven. Zo kunt u de geboorteplaats van één van uw kinderen nemen, of het model van de auto van de buren, of de kleur van uw huisdier.

Update uw software. Hackers maken gebruik van kwetsbaarheden die gevonden zijn in veelgebruikte software als besturingssystemen, kantoorproductiviteitssoftware en webbrowsers. Dit kunt u doen om dat te voorkomen:

- ◯ Installeer alle updates voor uw softwaretoepassingen en stel deze indien mogelijk zo in dat ze automatisch geüpdatet worden.
- ◯ Installeer anti-malwareprogramma's op alle computers. Als u verschillende computers in een netwerk hebt, gebruik dan software die beveiliging op ondernemingsniveau biedt en die updates beheert.

Blokkeer spam. Het is essentieel om een goede spamblocker te hebben. Spam is de meest gebruikte methode waarmee u het slachtoffer kunt worden van een infectie met een computervirus of van "social engineering". ("Social engineering" is als criminelen mensen psychologisch manipuleren zodat ze vertrouwelijke informatie verstrekken.)

2 Verhinder bedrog

Vermijd social engineering. Zelfs als u sterke wachtwoorden hebt, kunt u met trucs via social engineering worden overgehaald informatie te geven. Om dergelijke oplichting te voorkomen, dient u het volgende te onthouden:

- ◯ U moet nooit via e-mail of telefoon gevraagd worden om uw inloggegevens of persoonlijke gegevens te verstrekken. Geef die informatie dus niet, ook al lijkt de afzender legitiem.
- ◯ Zoek naar aanwijzingen die erop duiden dat een e-mail of website frauduleus is. Wees op uw hoede als u spelfouten ziet, koppelingen naar ongerelateerde sites of aanbiedingen die te mooi lijken om waar te zijn.

Pas op voor ransomware. Ransomware is een type malware dat bedoeld is om nietsvermoedende gebruikers te bedriegen. Het overtuigt u ervan dat uw computer geïnfecteerd is met een virus en dat u kosten moet betalen om software te downloaden waarmee uw computer gedesinfecteerd kan worden. Vertrouw op gerenommeerde beveiligingssoftware, zoals die van SOCIALware/TechSoup.

Surf veilig op het internet. Controleer of een website veilig en legitiem is voordat u financiële of persoonlijke gegevens invoert. Een veilige website heeft een URL die begint met **https**://. Op een veilige website kan bovendien de adresbalk een groene achtergrond hebben. (Of er wel of niet een groene achtergrond is, hangt af van de browser die u gebruikt.) Overweeg het gebruik van een afzonderlijke computer of gebruikersprofiel speciaal voor de financiële transacties van uw organisatie (zoals salarissen of donaties). Een speciale computer of gebruikersprofiel heeft idealiter minimale internettoegang en geen toegang tot e-mail.

3 Stel beleidsregels op voor medewerkers en vrijwilligers

Alle medewerkers en vrijwilligers zouden deze gids moeten lezen. Daarnaast dienen ze op de hoogte gebracht te worden van recent ontdekte beveiligingsrisico's. En verder:

- ◯ Stel een wachtwoordbeleid op voor uw organisatie en zorg ervoor dat medewerkers hun wachtwoorden geheim houden.
- ◯ Eventuele nieuwe medewerkers en vrijwilligers moeten getraind worden, zodat iedereen de risico's begrijpt en weet hoe die tot een minimum beperkt kunnen worden.
- ◯ Bepaal regels voor acceptabel gebruik van computers en mobiele apparaten, en vraag uw medewerkers te bevestigen dat ze deze gelezen hebben en begrijpen. In deze regels moet zijn vastgelegd wat gebruikers kunnen doen met de apparaten, wat erop geïnstalleerd en opgeslagen mag worden, en wat toegestaan is buiten de werkuren. De regels moeten ook betrekking hebben op het vervangen van verloren of gestolen apparaten.
- ◯ Verder kunt u overwegen om een discreet netwerk in te stellen en te ondersteunen, zoals een subnet of een draadloos netwerk voor "gasten" met strikte controles. Als dat niet haalbaar is, raden we meestal af om medewerkers of gasten hun eigen apparaten te laten gebruiken op het netwerk van uw organisatie. Laat u wel mensen op uw netwerk toe, implementeer dan een beleid dat passend is voor uw organisatie.

techsoup GLOBAL

4 Beveilig mobiele apparaten en externe werkstations

Laptops, tablets en telefoons worden gemakkelijk verloren of gestolen. Daarom geldt:

- Een mobiel apparaat mag nooit de enige locatie zijn waarop belangrijke gegevens worden bewaard.
- Net als bij computers op kantoor dient de toegang tot uw apparaat beschermd te worden met een PIN, wachtwoord of biometrie.
- Alle apparaten die zoek kunnen raken, dienen versleuteld te zijn. Deze voorzorgsmaatregel geldt ook voor laptops.
- Pas op voor malware, zoals kwaadaardige apps die bedoeld zijn om informatie te stelen. Bedenk u twee keer voordat u een app installeert en installeer alleen apps uit gerenommeerde appstores.
- Gebruik GPS- en locatiefuncties op uw telefoon of tablet alleen wanneer u ze nodig hebt. Het is waar dat deze mogelijkheid erg handig is voor persoonlijke doeleinden. Maar de locatiegegevens die worden opgenomen in uw statusupdates en foto's bieden hackers extra informatie die ze kunnen gebruiken voor social engineering.

Als uw apparaat verloren of gestolen is:

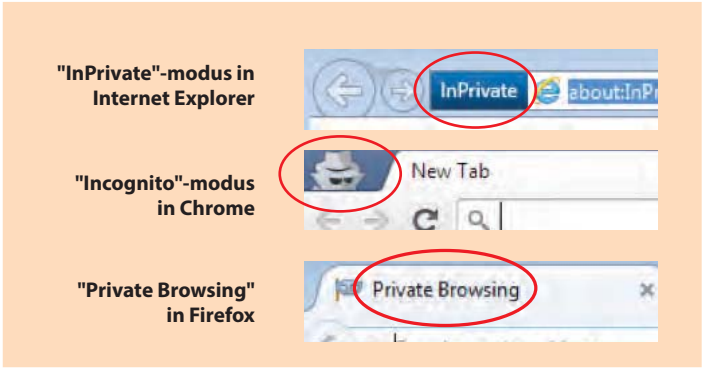
- U kunt het misschien terugvinden met de functie om een telefoon te zoeken.
- Als u het apparaat niet kunt vinden, kunt u wellicht op afstand alle gegevens wissen als het online is. Anders kunt u proberen alle gegevens op afstand te wissen als het apparaat weer online komt.

5 Wees voorzichtig als u openbare computers gebruikt

U moet elke openbare computer beschouwen als een veiligheidsrisico. Dat geldt ook voor openbare computers op luchthavens of in winkels, en voor computerlabs die openbare toegang bieden. Zulke computers zouden eigenlijk al in een "kioskmodus" moeten staan zodat er geen gegevens worden opgeslagen, maar ga er nooit vanuit dat dat ook inderdaad zo is.

Als u een openbare computer moet gebruiken:

- Gebruik deze nooit voor financiële transacties.
- Als u inlogt op e-mail of sociale media, gebruik dan de "privémodus" van de browser, zodat er geen informatie bewaard blijft nadat u de browser hebt afgesloten. Deze modus is toegankelijk vanaf de hoofdtaakbalk waar u normaal gesproken een nieuw tabblad of venster opent.



In openbare ruimtes moet u vooral ook letten op de fysieke beveiliging:

- Laat de computer nooit onbeheerd achter met gevoelige informatie op het scherm.
- Pas op voor mensen die over uw schouder meekijken.
- Sluit nooit uw apparaten of schijven aan op een openbare computer.

6 Wees voorzichtig als u openbare WiFi-netwerken gebruikt

U dient alle openbare WiFi-netwerken als onveilig te beschouwen. Dat betekent dat u:

- Openbare WiFi-netwerken alleen gebruikt voor niet-essentieel surfen op internet.
- Nooit financiële of persoonlijke transacties uitvoert via een openbaar netwerk.
- Veiliger alternatieven overweegt. Kijk of u iemand via de telefoon kunt spreken, of zelfs persoonlijk als hij of zij beschikbaar is.

Als u verbinding moet maken met een openbaar WiFi-netwerk:

- Maak verbinding met een netwerk dat enige vorm van beveiliging biedt in plaats van een "open" netwerk. Zo'n netwerk toont een "slot" of "schild" als symbool naast de netwerknaam. Bij veiliger netwerken moet u een wachtwoord invoeren of akkoord gaan met gebruiksvoorwaarden voordat u verder kunt.
- Pas op voor netwerken met vergelijkbare namen die bedoeld zijn om u om de tuin te leiden en te laten inloggen. Zulke netwerken kunnen uw dataverkeer afluisteren. Als u twijfelt, vraag dan aan iemand op die locatie om te controleren welk netwerk het juiste is.

Een virtual private network (VPN) kan helpen om sommige van deze risico's te verminderen wanneer u gebruik maakt van openbare netwerken. Als u medewerkers hebt die vaak op afstand werken of reizen, dan kunt u overwegen om een VPN op te zetten.

techsoup GLOBAL

7 Sociale media zijn sociaal (niet "privé")

Het is belangrijk om te begrijpen dat alles wat online is, zowel permanent als overdraagbaar is. Alles wat u op een sociale-mediasite doet, is ook toegankelijk voor adverteerders en is vaak meer openbaar toegankelijk dan u denkt.

Als u sociale media gebruikt, moet u altijd:

- ◯ Goed nadenken over hoe openbaar u wilt dat uw profiel en gegevens zijn.
- ◯ Elke site onderzoeken en evalueren —vooral de privacy-instellingen ervan— voordat u deze gaat gebruiken.
- ◯ Grenzen stellen aan wat u online wilt delen.
- ◯ Selectief zijn wanneer u mensen accepteert als "vrienden".
- ◯ Op uw hoede zijn als u persoonlijk afspreekt met iemand die u online hebt ontmoet, of dat nu om zakelijke of privéredenen is. Doe dat op een openbare locatie en laat anderen weten waar u naartoe gaat.

Sociale media zijn ook een populair startpunt voor phishing en social engineering. (Phishing is de poging om gevoelige informatie te verkrijgen, zoals gebruikersnamen, wachtwoorden en creditcardgegevens [en soms, indirect, geld]. De phisher doet zich in elektronische communicatie voor als een betrouwbare organisatie of persoon.) Dit komt doordat mensen van nature meer geneigd zijn te vertrouwen op wat hun "vrienden" plaatsen. Wees net zo voorzichtig als met e-mail en websites.

8 Beperk hoeveel u deelt

Persoonlijke gegevens kunnen worden gebruikt om u op te lichten, uw identiteit te stelen of u te vinden. Zaken die u online plaatst, kunnen in de toekomst ook invloed hebben bij het solliciteren, het aanvragen van kredieten of het afsluiten van verzekeringen en kunnen negatieve gevolgen hebben voor uw organisatie.

Om uw privacy, veiligheid en reputatie te beschermen als u sociale media gebruikt:

- ◯ Plaats alleen zaken waarvan u het niet erg vindt als die in het openbaar te horen zouden zijn.
- ◯ Plaats geen ongepaste foto's, video's of reacties.
- ◯ Als u een plaatsgebonden dienst gebruikt, overweeg dan om in te stellen wie toegang heeft tot die informatie. Informatie over uw locatie kan gemakkelijk gebruikt worden voor criminele doeleinden. Criminelen kunnen u bespioneren, u volgen of iets stelen.

9 Wees voorzichtig als uw organisatie gebruik maakt van sociale media

U dient vooral voorzichtig te zijn als medewerkers en vrijwilligers namens de organisatie gebruikmaken van sociale media. Net als bij beveiliging moeten nieuwe medewerkers en vrijwilligers die actief zullen zijn op sociale-mediakanalen begrijpen wat er van hen wordt verwacht.

- ◯ Medewerkers moeten zich ervan bewust zijn dat ze berichten of reacties plaatsen die in lijn zijn met de waarden van uw organisatie. U dient een sociale-mediabeleid te implementeren van uw organisatie.
- ◯ Als verschillende gebruikers een gedeeld account gebruiken, is het goed om vast te stellen welke medewerker dat doet en wanneer.
- ◯ Sommige diensten bieden verschillende rollen met verschillende gebruiksrechten. Wijs passende rollen toe aan medewerkers.
- ◯ Als u uw leden "tagt" of vermeldt in een bericht op sociale media, dan kunt u onbedoeld meer informatie over hen prijsgeven dan u zich realiseert. Wees dus voorzichtig met deze mogelijkheid.
- ◯ Tenzij u expliciet toestemming hebt van uw leden om beelden van hen te gebruiken, dient u hun gezichten onherkenbaar te maken in foto's en video's.

techsoup GLOBAL

10 Wees voorzichtig met inloggegevens en overweeg de toegang tot gedeelde bestanden te beperken

Als uw organisatie clouddiensten gebruikt, dan is de dienst toegankelijk voor iedereen die over de inloggegevens beschikt. Elke medewerker of vrijwilliger moet een unieke inlognaam hebben.

Veel diensten gebruiken tweeledige verificatie, waarbij de inloggegevens geverifieerd moeten worden via een tweede apparaat, zoals een mobiele telefoon. Schakel deze functie waar mogelijk in, vooral voor het maken van accountgerelateerde wijzigingen zoals wachtwoorden.

Gebruikers moeten ook voorzichtig zijn met wie ze toegang geven tot online documenten en bestanden. Online documenten en bestanden kunnen gemakkelijk gedeeld worden. Controleer de juistheid van e-mailadressen die gebruikt worden om toegang te geven en ga na of die persoon toestemming moet hebben om de content zowel te lezen als te bewerken.

11 Maak uzelf vertrouwd met het beleid van de aanbieder van de clouddiensten.

Als gebruiker van clouddiensten dient u op de hoogte te zijn van het beleid van de provider ten aanzien van eigendom en locatie van gegevens.

Als de autoriteiten gegevens opvragen, al de serviceprovider waarschijnlijk gehoor geven aan dat verzoek en uw gegevens aan hen overdragen. Als uw organisatie bezwaar zou maken tegen een overheidsbevel om uw gegevens over te dragen, dan is de cloud niet de juiste keuze. Gegevens in de cloud zijn ook een gemakkelijker doelwit voor uw tegenstanders.

Een "privé-" of "hybride" cloud kan voor u geschikter zijn dan de openbare cloud. Uw beslissing over die optie hangt af van de mate van exclusiviteit die uw organisatie vereist.

12 Bewaar offline back-ups

Wees erop voorbereid dat uw back-upservice niet beschikbaar is. Dat geldt voor zowel betaalde als gratis opties. Denk na over de gegevens die u in de cloud wilt bewaren en welke gevolgen het heeft op de bedrijfsvoering van uw organisatie als die informatie niet toegankelijk is.

Download kopieën van uw belangrijkste gegevens zodat u daar altijd toegang toe hebt, zelfs als de cloudservice niet beschikbaar is. Uw gegevens moeten geëxporteerd kunnen worden in een gangbaar formaat die u kunt gebruiken. Als dat niet het geval is, overweeg dan om over te stappen naar een provider die die mogelijkheid wel biedt.

Er is vaak een controlespoor van wijzigingen in online documenten. Controleer deze wijzigen van tijd tot tijd op ongebruikelijke activiteiten.

Maak veilig gebruik van de cloud

Het ontwerp en de vertaling van deze gids werden mede mogelijk gemaakt door de steun van Microsoft.