SANS SECURITY AWARENESS

De maandelijkse Security Awareness nieuwsbrief voor jou!

Veilig online winkelen

Overzicht

De feestdagen naderen en binnenkort zullen miljoenen mensen op zoek zijn naar de perfecte cadeaus. Op zoek naar geweldige aanbiedingen en om luidruchtige mensenmassa's te vermijden zullen velen online winkelen. Helaas zullen cybercriminelen ook actief zijn en valse winkelwebsites maken en andere tactieken gebruiken om mensen op te lichten. In deze nieuwsbrief leggen we uit hoe u veilig online kunt winkelen en voorkomen dat u het slachtoffer wordt.

Valse online winkels

Cybercriminelen creëren nepwebshops die het uiterlijk van echte sites nabootsen of die de namen van bekende winkels of merken gebruiken. Op zoek naar de beste online aanbiedingen, kunt u zich op een van deze nep-sites bevinden. Door van dergelijke websites te kopen, kunt u met nagemaakte of gestolen artikelen opgezadeld worden, en in sommige gevallen worden uw aankopen misschien nooit geleverd. Bescherm uzelf tegen namaakwebshops:

- Koop, indien mogelijk, bij de webwinkels die u al kent, vertrouwt en waarmee u al eerder zaken heeft gedaan. Plaats een bladwijzer bij online winkels die u eerder heeft bezocht en vertrouwt.
- Ben alert bij prijzen die beduidend lager zijn dan de prijzen die u ziet bij de gevestigde webwinkels. Als de deal te mooi klinkt om waar te zijn, kan het nep zijn.
- Let op wanneer de website lijkt op de website die u in het verleden hebt gebruikt, maar de domeinnaam van de website, of de naam van de winkel is net iets anders. U kunt bijvoorbeeld gewend zijn om te winkelen bij Amazon, waarvan het website-adres www.amazon.com is, maar uiteindelijk terechtkomen bij een nep-website die een vergelijkbaar website-adres heeft, maar de letter 'o' wordt vervangen door het nummer '0'.
- Typ de naam van de webwinkel of het webadres in een zoekmachine om te zien wat anderen erover hebben gezegd. Zoek naar termen als "fraude", "zwendel", "nooit meer" of "nep".
- Gebruik een uniek wachtwoord voor elk van uw online accounts. Kunt u zich niet al uw wachtwoorden herinneren? Overweeg ze allemaal op te slaan in een wachtwoordmanager.

Scammers op legitieme websites

Blijf op uw hoede, zelfs bij het winkelen bij vertrouwde websites. Grote webwinkels bieden vaak producten aan die verkocht worden door verschillende personen of bedrijven die mogelijk frauduleuze bedoelingen hebben. Dergelijke online bestemmingen zijn als echte markten, waar sommige verkopers betrouwbaarder zijn dan andere. Controleer de reputatie van elke verkoper voordat u de bestelling plaatst. Wees op uw hoede voor verkopers die nieuw zijn in de online winkel of die artikelen verkopen tegen ongewoon lage prijzen. Bekijk het beleid van de online winkel op aankopen van dergelijke derde partijen. Koop bij twijfel artikelen die rechtstreeks door de webwinkel worden verkocht en niet door derden die deelnemen aan de online marktplaats van de webwinkel.

Online betalingen voor aankopen

Controleer regelmatig uw creditcardafschriften om verdachte kosten te identificeren. Schakel, indien mogelijk, de optie in om u per e-mail, sms of app op de hoogte te stellen telkens wanneer er kosten van uw creditcard worden afgeschreven. Als u verdachte activiteiten aantreft, bel dan onmiddellijk uw creditcardmaatschappij en meld dit. Vermijd het gebruik van debetkaarten waar mogelijk. Betaalpassen nemen geld rechtstreeks van uw bankrekening af, als er fraude is gepleegd, heeft u het veel moeilijker om uw geld terug te krijgen. Een andere optie is het gebruik van bekende betalingsdiensten, zoals PayPal, voor online aankopen, die niet vereisen dat u uw creditcardnummer aan de verkoper bekendmaakt. Tot slot, overweeg het gebruik van een cadeaubon voor online aankopen.

Wanneer een online winkel een goed ontworpen, professionele uitstraling heeft betekent het niet automatisch dat deze legitiem is. Als de website u een ongemakkelijk gevoel bezorgt, gebruik hem dan niet. Ga in plaats daarvan naar een bekende site die u kunt vertrouwen en veilig heeft gebruikt in het verleden. Misschien vindt u die ongelofelijke deal niet, maar eindigt u wel met een legitiem product zonder te worden opgelicht.

Gastredacteur

Lenny Zeltser *is hoofd informatiebeveiliging bij Axonius en hoogleraar en auteur bij het SANS-instituut. Je kunt hem volgen op Twitter als @lennyzeltser en zijn blog lezen op zeltser.com.*

Bronnen

Social Engineering:	http://www.sans.org/u/X7k
Scamming You Through Social Media:	http://www.sans.org/u/X7p
Making Passwords Simple:	http://www.sans.org/u/Xu9