Maandelijkse Security Awareness nieuwsbrief voor Computergebruikers.

OUCH!

IN DEZE EDITIE...

Anderen Helpen Beveiligen

Overzicht

De meeste van ons zijn vertrouwd met technologie, ook om dit op een veilige manier te gebruiken. Sommige van onze vrienden en familieleden zijn minder vertrouwd. Ze kunnen er zelfs verward van raken of schrik krijgen. Dit maakt hen zeer kwetsbaar voor cyberaanvallers. Cyberbeveiliging hoeft niet angstaanjagend te zijn, het is eigenlijk eenvoudig eens je de basis begrijpt. Ze hebben enkel nood aan een gids die hen de basis laat begrijpen.

Gast redacteur

Randy Marchany (Twitter: @randymarchany) is de CISO van Virginia Tech en een gecertificieerde instructeur aan het SANS-Instituut.

Vijf Eenvoudige Stappen

Hier volgen vijf eenvoudige stappen die je kan nemen om anderen te helpen om veilig om te gaan met technologie. Voor meer informatie over elk van deze stappen, verwijzen we naar de Bronnen sectie aan het einde van deze nieuwsbrief.

1. **Social Engineering**: Social engineering is een veelgebruikte techniek van cyberaanvallers om mensen een bepaalde handeling te laten doen, zoals het delen van hun wachtwoord, computer besmetten of het delen van vertrouwelijke gegevens. Dit is niets nieuws, afpersers en oplichters bestaan sinds mensenheugenis. Het verschil is dat de slechteriken dezelfde methodes toepassen op het Internet. Je kan anderen helpen door hen uit te leggen welke kenmerken een social engineering aanval heeft, zoals situaties waarbij iemand een gevoel van urgentie creëert, wanneer iets té mooi is om waar te zijn of wanneer een cyberaanvaller zich voordoet als iemand die je kent maar de berichten van de persoon lijken niet op die van je normaal van die persoon ontvangt. Geef voorbeelden van veelgebruikte aanvallen, zoals phishingmails of de alombekende Microsoft tech support telefoons. Leer jouw familieleden dat ze nooit hun wachtwoord moeten geven aan iemand of zomaar toegang geven aan anderen tot hun computer.
2. **Wachtwoorden**: Sterke wachtwoorden zijn de sleutel tot het beschermen van toestellen en online accounts. Toon jouw familieleden hoe sterke wachtwoorden maken. We raden wachtzinnen aan, aangezien deze makkelijker zijn om te typen en te onthouden. Wachtzinnen zijn als wachtwoorden maar zijn gebaseerd op een zin. Help hen ook om een wachtwoordmanager te gebruiken. Hiermee kan je makkelijk een uniek wachtwoord voorzien voor elk toestel en account. Indien dit te veel is van het goede, geef dan de raad om de wachtwoorden neer te schrijven en de lijst op een veilige plaats te bewaren. Ten slotte is het belangrijk dat je hen helpt met twee-staps-verificatie in te schakelen (ook

Anderen Helpen Beveiligen

wel twee-factor-authenticatie genoemd). Twee-staps-verificatie is één van de beste maatregelen die je kan nemen om een account te beveiligen.

3. **Upgrades**: De laatste patches en upgrades toepassen is een belangrijke stap om jouw toestellen te beschermen. Dit geldt niet alleen voor jouw computers of mobiele toestellen, maar alles wat met het Internet kan verbinden zoals spelconsoles, thermostaten of zelfs luidsprekers en lichten. Schakel automatische updates in waar mogelijk, dit is de makkelijkste manier om al jouw toestellen bij te werken.
4. **Antivirus**: Mensen maken fouten, soms klikken we op of installeren we zaken die we beter niet doen omdat ze het systeem infecteren. Antivirus is er om je te helpen bij fouten. Antivirus kan echter niet alle malware stoppen, maar het helpt om de meest voorkomende aanvallen te detecteren en stoppen. Zorg ervoor dat jouw computers thuis een antivirus hebben en dat deze up-to-date en actief is. De meeste antivirusoplossingen van vandaag bevatten andere security technologie als firewalls en browserbescherming.
5. **Back-ups**: Back-ups zijn vaak de laatste oplossing om fouten te herstellen zoals het per ongeluk verwijderen van bestanden of cyberaanvallen zoals ransomware. Zorg ervoor dat familie en vrienden een automatisch back-upsysteem hebben. Vaak zijn de eenvoudigste oplossingen deze in de Cloud. Deze oplossingen nemen een back-up, ieder uur of telkens wanneer je een bestand wijzigt. Ze maken het eenvoudig om een back-up te nemen maar ook om bestanden te herstellen.

Deel deze vijf eenvoudige stappen zodat anderen veilig omgaan met de laatste technologieën.

Kinderen Op Bezoek Beschermen

Als je vertrouwd bent met technologie, heb je allicht niet alleen jezelf goed beschermd maar ook jouw kinderen. Als jouw kinderen op bezoek gaan bij iemand die niet vertrouwd is met technologie, bijvoorbeeld de grootouders, weten deze vrienden of familie niet hoe ze best kinderen online beschermen. Hier zijn enkele stappen die je kan nemen om kinderen te beschermen wanneer ze, vooral bij familie, op bezoek zijn:

- **Regels**: Zorg ervoor dat je regels of verwachtingen bepaalt voor de online veiligheid van jouw kinderen en dat anderen deze weten. Bijvoorbeeld zijn er regels voor hoe lang kinderen online mogen zijn, met wie ze mogen praten of welke spellen ze mogen en niet mogen spelen? Let op dat je er niet op vertrouwt dat de kinderen de regels uitleggen tegen de familieleden. Een goed idee is om een papier met regels op te maken en deze te geven aan het familielid waar men blijft.

Anderen Helpen Beveiligen

- **Controle**: Als een kind beter overweg kan met technologie dan zijn oppas, dan kunnen ze dit 'creatief' gaan gebruiken. Zo kan het kind bijvoorbeeld vragen achter beheerrechten op de computer van de grootouders om te doen wat ze willen. Zoals het installeren van een spel dat ze niet mogen spelen. Zorg ervoor dat jouw familie begrijpt dat ze kinderen geen extra toegang mogen geven.

Ten slotte, raad mensen aan om zich in te schrijven op nieuwsbrieven zoals de OUCH! Nieuwsbrief, zodat ze meer kunnen leren. Deze nieuwsbrief wordt iedere maand gratis in 20 verschillende talen uitgebracht. Schrijf je in via https://securingthehuman.sans.org/ouch.

Meer Weten?

Ga naar securingthehuman.sans.org/ouch/archives om je te abonneren op de maandelijkse OUCH! Security awareness nieuwsbrief, toegang te krijgen tot het OUCH! archief en kom meer te weten over SANS security awareness oplossingen.

Over Cegeka Groep

Cegeka is een onafhankelijke ICT–dienstverlener die klanten in heel Europa helpt met hun digitale transformatie, agile ontwikkeling, trusted cloudoplossingen en 24/7 managed services. Cegeka heeft vestigingen in België, Duitsland, Frankrijk, Italië, Nederland, Luxemburg, Oostenrijk, Polen, Roemenië, Slowakije en Tsjechië. Cegeka heeft 3.600 medewerkers. In 2015 realiseerde Cegeka Groep een omzet van 368 miljoen euro. Bezoek www.cegeka.com voor meer informatie.

Bronnen

Social Engineering:	https://securingthehuman.sans.org/ouch/2017#january2017
Passphrases:	https://securingthehuman.sans.org/ouch/2017#april2017
Password Manager:	https://securingthehuman.sans.org/ouch/2017#september2017
Two-Step Verification:	https://securingthehuman.sans.org/ouch/2015#september2015
Backup and Recovery:	https://securingthehuman.sans.org/ouch/2017#august2017
Securing Today's Online Kids:	https://securingthehuman.sans.org/ouch/2017#may2017

Redactie: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Vertaald door: Sven Jacobs, Tom Palmaers

securingthehuman.sans.org/blog /securethehuman @securethehuman securingthehuman.sans.org/gplus