De maandelijkse Security Awareness nieuwsbrief voor jou!

Vier eenvoudige stappen voor uw veiligheid

Overzicht

Veilig en zeker gebruik maken van technologie kan overweldigend en verwarrend lijken. Echter, ongeacht welke technologie je gebruikt of hoe je deze gebruikt zijn hier vier eenvoudige stappen die zullen helpen om veilig te blijven.

1. JIJ: In de eerste plaats kan technologie alleen je niet volledig beschermen, jij bent jouw beste verdediging. Aanvallers hebben geleerd dat de gemakkelijkste manier om te krijgen wat ze willen is om zich te richten op jou, in plaats van jouw computer of andere apparaten. Als ze je wachtwoord, creditcard of controle over jouw computer willen, zullen ze proberen je te verleiden om het aan hen te geven, vaak door een gevoel van urgentie te creëren. Ze kunnen je bijvoorbeeld bellen terwijl ze zich voordoen als Microsoft tech support en beweren dat jouw computer geïnfecteerd is, terwijl het in werkelijkheid slechts cybercriminelen zijn die willen dat jij hen toegang tot jouw computer geeft. Of misschien sturen ze een e-mail met een waarschuwing dat jouw pakket niet kon worden afgeleverd en zetten ze je onder druk om op een link te klikken om jouw postadres te bevestigen, terwijl ze je in werkelijkheid voor de gek houden om een kwaadaardige website te bezoeken die jouw computer zal hacken. Uiteindelijk ben jij de grootste verdediging tegen aanvallers. Door gebruik te maken van gezond verstand kun je veel aanvallen herkennen en stoppen.

2. Passphrases: Moderne computersnelheden hebben het oude, 8-karakterige wachtwoord verouderd en kwetsbaar gemaakt. Wanneer een site vraagt om een wachtwoord aan te maken, maak dan in plaats daarvan een sterke en unieke passphrase aan. Een passphrase is een type wachtwoord dat een reeks gemakkelijk te onthouden woorden gebruikt, zoals “bee honey bourbon rain”. Hoe langer de passphrase is, hoe sterker. Een unieke passphrase betekent dat je voor elk apparaat of online account een andere passphrase gebruikt. Op deze manier zijn al jouw andere accounts en apparaten nog steeds veilig als één passphrase gecompromitteerd is. Kun je je al die wachtwoordzinnen niet herinneren? Gebruik een wachtwoordmanager, een gespecialiseerd programma dat al jouw wachtwoordzinnen veilig opslaat in een versleuteld formaat (en nog veel meer geweldige functies).

Schakel tot slot verificatie in twee stappen in (ook wel two-factor of multi-factor authenticatie genoemd). Het gebruikt jouw wachtwoord, maar voegt ook een tweede stap toe, zoals een code die naar de smartphone wordt gestuurd of een app die de code voor je genereert. Verificatie in twee stappen is waarschijnlijk de

belangrijkste stap die je kunt nemen om jouw online accounts te beschermen en het is veel gemakkelijker dan je misschien denkt.

3. Updaten: Zorg ervoor dat al jouw computers, mobiele apparaten, programma's en apps de nieuwste versie van de software gebruiken. Cyberaanvallers zijn voortdurend op zoek naar nieuwe kwetsbaarheden in de software die jouw apparaten gebruiken. Wanneer ze kwetsbaarheden ontdekken, gebruiken ze speciale programma's om deze te misbruiken en in te breken in de apparaten die je gebruikt. Ondertussen zijn de bedrijven die de software voor deze apparaten hebben gemaakt, hard aan het werk om ze te repareren door updates vrij te geven. Door ervoor te zorgen dat jouw computers en mobiele apparaten deze updates snel installeren, maak je het veel moeilijker voor iemand om jou te hacken. Om op de hoogte te blijven, schakel je eenvoudigweg automatisch updaten in wanneer dat mogelijk is. Deze regel is van toepassing op bijna elke technologie die op een netwerk is aangesloten, waaronder tv's met internetverbinding, babyfoons, beveiligingscamera's, thuisrouters, spelconsoles of zelfs jouw auto.

4. Back-ups & Recovery: Soms, hoe voorzichtig je ook bent, kun je gehackt worden. Als dat het geval is, is de enige manier om al jouw persoonlijke informatie te herstellen vaak de back-up. Zorg ervoor dat je regelmatig back-ups maakt van alle belangrijke informatie en controleer of je jouw gegevens kunt herstellen. De meeste besturingssystemen en mobiele apparaten ondersteunen automatische back-ups, zowel op externe schijven als op de cloud.

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 meer dan 4.200 medewerkers. In 2018 realiseerde Cegeka Groep een omzet van 512 miljoen euro. Bezoek www.cegeka.com voor meer informatie.

Gastredacteur

*SANS Certified Instructor **Steve Anson** biedt begeleiding aan IT-beveiligingsteams en overheden over de hele wereld om hun veiligheidspositie te verbeteren. Steve is de auteur van het aankomende boek Applied Incident Response en biedt gratis bronnen voor IT-beveiligingsmedewerkers op www.AppliedIncidentResponse.com.*

Bronnen

Social Engineering: https://www.sans.org/u/W3G
Personalized Scams: https://www.sans.org/u/W3Q
Making Passwords Simple: https://www.sans.org/u/W3V
Got Backups: https://www.sans.org/u/W40