CYBERSECURITY AWARENESS MONTH

ZIE JEZELF IN CYBER (SEE YOURSELF IN CYBER)

Iedereen speelt een rol in cyberbeveiliging... ongeacht je rol.

Doe je deel om jezelf en ons bedrijf veilig te houden op het gebied van cyberbeveiliging door de volgende vier belangrijke acties te volgen.

SCHAKEL MULTIFACTORAUTHENTICATIE IN

Ook wel tweefactorauthenticatie en verificatie in twee stappen genoemd, multifactorauthenticatie is een veiligheidsmaatregel die vereist dat iedereen die zich aanmeldt op een account een procedure volgt die bestaat uit twee stappen om zijn of haar identiteit te bevestigen. Dit maakt het dubbel zo moeilijk voor criminelen om toegang te krijgen tot een online account. Door een extra eenvoudige stap toe te voegen bij het aanmelden op een account, verhoogt multifactorauthenticatie de beveiliging van je account aanzienlijk.

GEBRUIK STERKE WACHTWOORDEN

Wachtwoorden zijn belangrijk als je wilt dat je informatie veilig blijft. Hier vind je een aantal eenvoudige manieren om je accounts te beveiligen met behulp van betere wachtwoordpraktijken. Ongeacht om welk account het gaat, creëer alle wachtwoorden met deze drie woorden in gedachte.

- Lengte – Tenminste 12 tekens
- Uniek – Elk account heeft zijn eigen unieke wachtwoord nodig
- Complex – Gebruik een combinatie van grote en kleine letters, cijfers en speciale tekens. Op sommige websites kun je zelfs spaties gebruiken.

SOFTWARE UPDATEN

Zorg ervoor dat je je software altijd updatet wanneer nieuwe updates beschikbaar zijn en stel dit niet uit. Deze updates lossen algemene softwareproblemen op en bevatten nieuwe beveiligingspatches op plaatsen waar criminelen kunnen binnendringen. Als je een software-update downloadt, haal deze dan alleen bij het bedrijf dat deze heeft gemaakt. Gebruik nooit gehackte, vervalste versies of versies van software zonder licentie aangezien deze vaak malware bevatten en meer problemen veroorzaken dan dat ze oplossen.

HERKEN EN RAPPORTEER PHISHING

De tekenen kunnen subtiel zijn, maar wanneer je een phishing-poging herkent, kun je vermijden om erin te trappen. Hier vind je wat snelle tips om een nep phishing-mail duidelijk te herkennen: deze mails bevatten vaak een aanbieding die te mooi is om waar te zijn; taal die dringend, alarmerend of bedreigend is; ze zijn slecht geschreven en bevatten vaak grammaticale en spellingsfouten; de begroeting is dubbelzinnig of zeer algemeen; verzoeken om persoonlijke informatie te sturen; urgentie om op onbekende hyperlinks of bijlage te klikken; rare of abrupte zakelijke verzoeken; het e-mailadres stemt niet overeen met het bedrijf die de mail heeft verzonden.

MAUSER
Packaging Solutions