Gemeente Rotterdam

Digitaal Veilig

Informatieblad

Januari 2020

We zijn steeds meer actief op internet. Dit biedt kansen, maar helaas zijn er ook mensen die er misbruik van maken. Criminaliteit via internet neemt toe, waarbij iedereen slachtoffer kan worden. Phishing, gijzelsoftware, oplichting en spam kunnen grote schade aanbrengen. In dit informatieblad treft u de belangrijkste en eenvoudige maatregelen aan die u kunt treffen om uzelf en anderen te beschermen.

Installeer een antivirusprogramma

Gebruik een antivirusprogramma om uw computer, tablet en smartphone te beschermen en schakel automatische updates in. Laat het antivirus-programma daarnaast geregeld uw apparaten scannen op infecties, bijvoorbeeld iedere maand. Schakel een eventueel meegeleverde firewall altijd in, zodat het de verbindingen tussen het apparaat en het internet in de gaten kan houden.

Gebruik sterke wachtwoorden

Het gebruiken van een moeilijk te raden wachtwoord is belangrijk, vooral bij cruciale systemen zoals DigiD of uw wifinetwerk. Gebruik daarnaast voor elke dienst een uniek wachtwoord. Hiervoor kunt u gebruik maken van een wachtwoordmanager, die unieke wachtwoorden kan genereren en opslaan. Waar mogelijk gebruikt u tweestapsverificatie om uw account extra te beschermen.

Installeer steeds de software-updates

Producenten van besturingssystemen, browsers en andere programma's, zoals Microsoft Office, Adobe Reader en Oracle Java, brengen geregeld updates uit om beveiligingslekken te verhelpen. Maak ook hier waar mogelijk gebruik van automatische updates. Controleer in andere gevallen minimaal maandelijks of updates beschikbaar zijn en installeer deze.

Open geen berichten en onbekende bestanden die u niet verwacht of niet vertrouwt

Ontvangt u onverwacht een bericht met een bijlage, (ingekorte) hyperlink of verzoek om in te loggen op een systeem? Gebruik uw gezond verstand en ga hier niet op in, zelfs niet wanneer u de afzender kent. Accepteer het bericht alleen als u het van deze afzender verwachtte te krijgen. Spam verwijdert u het beste direct.

Installeer alleen apps via de officiële applicatiewinkels

Ook apps voor uw smartphone of tablet kunnen malware bevatten. Installeer apps daarom alleen via de officiële applicatiewinkels en gebruik geen illegale kopieën. Kijk ook goed naar de toegangsrechten van de app. Bekijk ervaringen van medegebruikers om u een beeld te vormen van de betrouwbaarheid van de app.

Controleer het adres van websites

Controleer het webadres (URL) en het certificaat (het hangslotje in de adresbalk van de browser) om vast te stellen dat u geen nagemaakte of onveilige website bezoekt. Is er geen hangslotje? Vul dan geen gevoelige gegevens in op deze website. Gebruik bladwijzers voor websites die u vaak bezoekt en let extra op bij het openen van verkorte URLs. Deze worden veel gebruikt op sociale netwerken.

Ongevraagd helpdesk-advies: verbreek de verbinding

Oplichters die zich voordoen als medewerkers van IT-bedrijven zoals Microsoft, proberen u telefonisch wijs te maken dat u een computerprobleem heeft, maar dat daar (tegen een vergoeding) iets aan te doen is. Vervolgens vraagt de oplichter om hem mee te laten kijken in uw computer, waardoor hij bijvoorbeeld bij uw bankrekening kan komen. Of hij vraagt betaling voor zijn diensten, bijvoorbeeld via Western Union of Moneygram. Krijgt u zo'n telefoontje, ga dan niet met deze mensen in gesprek. Gerenommeerde bedrijven zoals Microsoft bellen nooit met dit soort meldingen.

Bedenk goed wat u met wie deelt op internet

Zo gemakkelijk als het is om iets op internet te plaatsen, zo moeilijk is het om dit er weer af te krijgen. Denk dus goed na over wat u wel of niet op internet wilt delen. Scherm uw sociale netwerksites goed af en wees selectief in wie toegang krijgt tot uw profiel en gegevens. Laat u uw gegevens ergens achter, ga dan na bij welke organisatie u dat doet, hoe lang uw gegevens worden bewaard en aan wie deze nog meer kunnen worden verstrekt. Geef niet meer gegevens dan noodzakelijk is.

Maak regelmatig back-ups

Door regelmatig back-ups te maken van uw computer en van uw bestanden of foto's op uw telefoon of tablet, kunt u schade van bijvoorbeeld gijzelsoftware of virussen beperken. Indien u een back-up heeft liggen, kunt u toch nog bij een kopie van uw gegevens. Back-ups maakt u op externe, losgekoppelde gegevensdragers (zoals een DVD, USB-stick of externe harde schijf) die u op een andere locatie bewaart. Ook kunt gebruik maken van een online-opslagdienst.

Gebruik uw gezond verstand

Als iets te mooi lijkt om waar te zijn, dan is het dat meestal ook. Wees alert als u iets niet vertrouwt of niet kent.

Maak alleen verbinding met vertrouwde wifinetwerken

Bij openbare en onbeveiligde wifinetwerken kunnen anderen mogelijk zien wat u op het internet doet en welke gegevens u verstuurt. Verstuur dus geen gevoelige gegevens (e-mail, internetbankieren) over netwerken die u niet kent of niet vertrouwt. Versleutel thuis uw draadloze netwerk met WPA2 met AES-encryptie om te voorkomen dat kwaadwillenden uw internetverkeer kunnen onderscheppen.

Ga naar www.rotterdam.nl/cyber voor meer informatie!