Vier tips voor een veiliger internetgebruik

Iedereen is tegenwoordig online. We shoppen online, laten de mooiste kant van ons leven zien op Instagram, versturen ook nog steeds veel e-mail en leren de nieuwste dansmoves op TikTok. Bovendien zijn we voor meer serieuze zaken zoals internetbankieren, verzekeringen en contact met de overheid ook volledig afhankelijk geworden van het internet. Veel mensen zijn zich onvoldoende bewust van de risico's die zij lopen op het internet en hebben het idee dat zij totaal oninteressant zijn voor cybercriminelen (internetcriminelen).

Maar ook cybercriminelen zijn bekend met dit fenomeen. Moest er vroeger nog echt worden ingebroken in een woning om toegang te krijgen tot geld of bankgegevens. Nu is een online account al voldoende om iemands digitale identiteit volledig over te kunnen nemen.
Stel je eens voor wat een cybercrimineel allemaal op jouw naam kan doen wanneer hij/zij toegang heeft tot bijvoorbeeld jouw e-mail adres.

In dit blog geven we je vier tips mee waarmee jij je online identiteit beter kunt beveiligen en met een geruster hart online kunt shoppen, internetbankier of TikTokken:

- **Gebruik voor ieder account een uniek wachtwoord en maak deze zo lang mogelijk**
- **Maak gebruik van een wachtwoordmanager om deze wachtwoorden te onthouden**
- **Gebruik Tweetrapsverificatie wanneer dit beschikbaar is**
- **Installeer updates**

Gebruik voor ieder account een uniek wachtwoord en maak deze zo lang mogelijk

Gebruikersnamen en wachtwoorden zijn de toegangspoort tot jouw online identiteit en accounts. Wanneer je voor al je accounts dezelfde inloggegevens gebruikt is de kans groot dat deze gegevens ooit eens bij internetcriminelen bekend worden. Doordat je dan op alle accounts dezelfde gegevens gebruikt heeft die internetcrimineel (of de criminelen aan wie hij/zij jouw gegevens verkoopt) direct toegang tot al jouw accounts.

Wanneer je voor ieder account een uniek wachtwoord instelt dan heeft een internetcrimineel alleen toegang tot dat account, mocht het account ooit gehackt worden, en niet tot al jouw accounts.
Door op ieder account een uniek wachtwoord in te stellen beperkt je dus de risico's en bescherm je jouw online identiteit veel beter.

Met speciale software proberen internetcriminelen wachtwoorden te kraken. Hoe langer een wachtwoord is en hoe meer verschillende tekens een wachtwoord bevat hoe langer het duurt voordat een wachtwoord is gekraakt. Heeft zo'n programma maximaal 8 uur nodig om een wachtwoord van 8 karakters te kraken, datzelfde programma doet er 2 miljoen jaar over om een wachtwoord van 14 karakters (die is voorzien van hoofdletters, kleine letters, cijfers en vreemde tekens). In het geval van wachtwoorden is lengte dus echt van belang.

Maak gebruik van een wachtwoordmanager

Al die verschillende wachtwoorden onthouden is natuurlijk niet te doen. Onze tip hiervoor is: maak gebruik van een wachtwoordmanager. Een wachtwoordmanager is een beveiligde kluis waarin je al jouw wachtwoorden opslaat. Deze kluis beveilig jij met een goed (dus lang, uniek) wachtwoord en **tweetrapsverificatie** zodat alleen jij toegang hebt tot jouw wachtwoordenkluis.

Veel wachtwoordmanagers kunnen worden gekoppeld aan de browser op jouw computer zodat je vanuit de wachtwoordmanager direct, veilig, toegang hebt tot al jouw accounts. Ook hebben de meeste wachtwoordmanagers een goede en veilige app beschikbaar zodat jij je accounts ook altijd veilig bij je hebt op je smartphone.

Maak je gebruik van een wachtwoordmanager dan hoef je dus zelf nog maar één wachtwoord te onthouden. De rest van de gegevens zijn veilig voor je opgeslagen in je wachtwoordenkluis die je hebt beveiligd met tweetrapsverificatie.

Tip: de meeste wachtwoordmanagers hebben ook een wachtwoordgenerator beschikbaar. Hiermee creëer je snel en eenvoudig lange en veilige wachtwoorden die je direct kunt opslaan in je wachtwoordmanager.

Gebruik Tweetrapsverificatie

Bij het gebruik van Tweetrapsverificatie (ook wel Multifactor Authenticatie) wordt er twee keer aan jou gevraagd om aan te tonen dat jij ook daadwerkelijk jij bent. Doorgaans meld je op een account aan met je gebruikersnaam (vaak e-mailadres) en wachtwoord. Tweetrapsverificatie voegt daar een extra methode aan toe. Vaak wordt dit gedaan in combinatie met een app op je smartphone waaruit je een code dient over te nemen of een melding dient te accepteren.

Dat klinkt omslachtig en vervelend maar zorgt ervoor dat internetcriminelen haast geen kans maken om toegang te krijgen tot jouw online accounts. Ze dienen immers al toegang te hebben tot jouw gebruikersnaam en wachtwoord maar hebben daarnaast ook nog jouw smartphone nodig om daadwerkelijk toegang te kunnen krijgen tot jouw online accounts.

Heb je tweetrapsverificatie op een account die je dagelijks gebruikt? Dan is er vaak de mogelijkheid om de tweetrapsverificatiemelding bijvoorbeeld op één specifieke computer maar één keer per maand te laten verschijnen. Hierdoor blijft je account toch veilig maar ondervind je minder ‘hinder’ van tweetrapsverificatie.

Veel grotere diensten en webshops bieden al standaard tweetrapsverificaties aan. Maak daar dan ook gebruik van! Vraag je ICT-beheerder of ICT-partner of tweetrapsverificatie ook op jouw accounts kan worden ingeschakeld.

Installeer updates

Last but not least: Installeer updates!

Softwareleveranciers brengen regelmatig updates uit voor hun programma's. Deze updates bevatten vaak beveiligingsupdates waarmee lekken in het programma worden gedicht. Internetcriminelen maken actief misbruik van deze lekken in programma's en software.

Controleer dus regelmatig op updates en installeer deze. Nog beter is het om het automatisch updaten van je smartphone of computer in te schakelen. Je krijgt dan vanzelf melding wanneer er een update geïnstalleerd kan worden en hebt er zelf geen omkijken meer naar.

Een up-to-date computer of smartphone is van cruciaal belang om veilig te kunnen werken. Installeer dan ook updates zodra deze beschikbaar komen.

Conclusie

Door gebruik te maken van redelijk eenvoudige maatregelen kun je jouw online identiteit goed beschermen. Dus installeer updates, gebruik overal unieke wachtwoorden en sla deze op in een wachtwoord manager en gebruik tweetrapsverificatie wanneer het beschikbaar is. Natuurlijk zijn er nog veel meer andere maatregelen die je zou kunnen nemen maar wanneer je bovenstaande stappen allemaal hebt doorgevoerd dan heb je al een flinke stap gezet in jouw online veiligheid.

Begin nu, voordat je gegevens wel op straat liggen!

Heb je vragen over één van bovenstaande onderwerpen of wil je graag weten wat jij in jouw specifieke situatie kunt doen om jouw accounts beter te beveiligen? Neem dan contact met ons op via info@acfbentveld.nl of 0527-858585.