Kristien Piersma / k.i.piersma@rug.nl

TIPS

Be safe: bewust van de gevaren op internet

Om gebruikers meer bewust te maken van de veiligheidsgevaren die internet met zich meebrengt, is SURFnet van start gegaan met de beveiligingscampagne Cybersave Yourself. Tijdens de campagne staan de thema's phishing, social media, vertrouwelijke informatie en mobile computing centraal.

We doen steeds meer online: van mailen en bankieren tot het onderhouden van sociale contacten. Dat betekent ook dat er steeds meer accountgegevens onthouden moeten worden. Ook laten we steeds vaker gegevens van onszelf achter op het internet wanneer bijvoorbeeld aankopen worden gedaan, afspraken worden gemaakt of bij het aanvragen van informatie. Hoe kan worden voorkomen dat deze persoonsgegevens worden misbruikt? Hoe kunt u uw identiteit goed afschermen?

De pc beveiligen

Het beveiligen van de computer is tegenwoordig een must. Wanneer dat niet goed gebeurt, kunnen onbevoegden toegang krijgen tot uw pc. Alles wat op de computer staat, zoals persoonlijke documenten en foto's, en alles wat u op uw computer heeft gedaan, is dan door onbevoegden in te zien en te manipuleren.

Door aandacht te besteden aan het beveiligen van de computer kan worden voorkomen dat bijvoorbeeld bestanden op uw computer door virussen worden beschadigd of verwijderd, dat uw computer gebruikt wordt door kwaadwillenden om bijvoorbeeld spam mee te versturen of dat gegevens op uw computer gestolen en misbruikt kunnen worden.

Op de website Cybersave Yourself is meer informatie te vinden over het gebruik van firewalls, virusscanners en windows updates.

Databeveiliging

Op de gemiddelde pc van tegenwoordig staan een hoop gegevens waarvan het niet de bedoeling is dat ze in verkeerde handen vallen. Vreemden kunnen de gegevens opzettelijk veranderen, verwijderen of voor eigen doeleinden gebruiken. Maar er kan ook iets mis gaan met de pc waarbij

vervolg van pagina 15 Helpdesk

de gegevens kunnen worden gewist door een virus of de harde schijf beschadigd raakt.

U kunt zelf eenvoudig maatregelen nemen om te voorkomen dat onbevoegden toegang tot uw data krijgen of dat u uw data kwijt raakt. Maak bijvoorbeeld regelmatig back-ups op externe gegevensdragers zoals een CD, DVD, USB-stick of externe harde schijf. Wanneer u even wegloopt van uw pc, maak er dan een gewoonte van dat u uitlogt of de pc vergrendelt. Een handige toetsencombinatie voor het vergrendelen van de pc is de toets met het Windows-logo in combinatie met de letter L.

Mocht uw USB-stick in verkeerde handen vallen, zorg er dan voor dat hij zo beveiligd is dat niemand iets met de gegevens kan doen. Er zijn gratis programma's die kunnen worden gebruikt om een USB-stick te versleutelen en alleen toegang te verlenen als het juiste wachtwoord ingevuld is. Meer informatie hierover is te vinden op de Cybersave Yourself-website. Ook wordt in dit verband aandacht besteed aan het gebruik van draadloze netwerken, het beveiligen van mobiele apparaten zoals laptops, pda's, tablet pc's en mobiele telefoons.

Wachtwoordbeleid

Wachtwoorden fungeren (in combinatie met een gebruikersnaam) als sleutels om toegang te krijgen tot persoonlijke informatie op de computer en online-diensten. Het is dus van belang uw wachtwoord goed te kiezen en ook geheim te houden. In handen van de verkeerde persoon kunnen er vervelende dingen gebeuren: het online chatten of mailen vanuit uw naam (waarbij uw vrienden kunnen worden lastig gevallen) maar ook het met de verkregen gegevens afsluiten van leningen. U komt er vaak pas achter als het al te laat is...

Een paar tips om veilig met uw wachtwoord om te gaan:

- Geef uw wachtwoord aan niemand, ook niet aan mensen die u kent en/of vertrouwt.
- Zorg dat er niemand met u meekijkt als u uw wachtwoord intypt.
- Vervang uw wachtwoord zo nu en dan voor een ander wachtwoord (bijvoorbeeld iedere paar maanden): naarmate u een wachtwoord langer in gebruik heeft, neemt de kans toe dat iemand achter uw wachtwoord is gekomen.
- Laat uw wachtwoord niet rondslingeren in de buurt van uw computer, op uw bureau of in uw agenda.
- Wanneer er een venster wordt geopend waarin u wordt gevraagd of uw computer het wachtwoord voor de betreffende site moet opslaan, kies dan 'Nee'. Met deze optie kan iedereen die van uw computer gebruik maakt, uw opgeslagen wachtwoorden voor deze sites gebruiken.
- Gebruik niet voor alles hetzelfde wachtwoord, maar verzin voor al uw online-activiteiten een nieuw wachtwoord.
- Geef uw wachtwoord nooit via de e-mail, ook niet wanneer het verzoek van een betrouwbaar bedrijf of persoon komt.

Sterk wachtwoord

Door een sterk wachtwoord te bedenken en er veilig mee om te gaan, kunt u uw informatie beschermen. Sterke en dus veilige wachtwoorden bestaan uit minimaal acht karakters, bevatten cijfers, hoofdletters en kleine letters en speciale tekens. Sterke wachtwoorden bevatten geen hele woorden, logische volgordes of opvolgende nummers.

U kunt dus wel woorden of namen in uw wachtwoord gebruiken, maar zorg er dan voor dat het woord of de naam onderbroken wordt door een getal of een speciaal teken.

Beveiligen van de identiteit

Veel mensen hebben niet alleen in de echte wereld een identiteit, maar ook op het internet. Er wordt dan ook wel gesproken van een *digitale* of *virtuele* identiteit. Doordat men op het internet op veel plekken persoonlijke informatie achterlaat, op waarheid gebaseerd of niet, wordt op het internet een (of meerdere) identiteit(en) gecreëerd. Deze identiteit is, zonder dat u daar zelf goed zicht op heeft, in te zien door andere internetgebruikers. Onbekenden kunnen zo van alles over u te weten komen. Ga daarom veilig om met persoonlijke gegevens die u op het internet achterlaat.

Surf bewust

Hoe vaak wordt u op het internet niet gevraagd om een account aan te maken? Even snel een wachtwoord bedenken en u staat weer geregistreerd. Op talloze websites worden zo sporen achtergelaten, denk maar aan vriendensites, discussiefora, prijsvragen, persoonlijke zoekmachines, chatrooms, youtube et cetera. En ook al laat u geen e-mailadres achter, uw bezoek is alsnog te achterhalen.

Let dus op wat u op het internet doet en welke (persoonlijke) gegevens u achterlaat. Soms is inloggen nodig of moet u gegevens invoeren, bijvoorbeeld bij het internetbankieren of wanneer u online iets koopt. Controleer altijd of u een veilige verbinding heeft en of u op de juiste website (URL) zit.

Reageer nooit op spam

Spam is irritant en voor criminelen nog steeds lonend. Activeer daarom een spamfilter. Volg hiervoor de instructies op van uw provider of van de beheerder van de werkplek. Het spamfilter selecteert spamberichten en stopt ze in een aparte folder. Laat u nooit verleiden te reageren op deze e-mails. Antwoord nooit, maar gooi ze weg. Wees ook spaarzaam met het achterlaten van uw e-mailadres op websites! Dit voorkomt het ontvangen van spam.

Phishing

Phishing is een vorm van digitaal oplichten onder andere door het sturen van foutieve links of e-mails, vaak vol met grammatica- en spelfouten. Meestal wordt hierbij op slinkse wijze naar inloggegevens, bankgegevens of creditcard gegevens gevraagd. Criminelen proberen op deze manier u te verleiden om persoonlijke gegevens af te geven. Een betrouwbare organisatie zal nooit op eigen initiatief om uw persoonlijke gegevens vragen. Reageer dus niet.

- Meer informatie over de campagne van SURFnet: **www.cybersaveyourself.nl**
- Informatie over veilig internetbankieren: **www.3xkloppen.nl**
- Website van het ministerie van Justitie met tips om veilig te internetten **www.nederlandveilig.nl/veiliginternetten**
- Website waar waarschuwingen worden gegeven indien er dreigingen zijn op het internet: **www.waarschuwingsdienst.nl**