Matto Fransen / m.j.fransen@rug.nl

Bescherm uw account

Matto Fransen is security manager bij het CIT. Met deze functie probeert de RUG het 'security bewustzijn' bij de gebruikers van de universitaire ICT-voorzieningen te bevorderen.

Het account dat u bij de universiteit heeft, is een persoonlijk account. De gebruikersnaam en het wachtwoord zijn de sleutel om toegang te krijgen tot eigen en gedeelde bestanden en systemen zoals e-mail. Het is zaak daar zorgvuldig mee om te gaan, net als bijvoorbeeld met het account waarmee u telebankiert.

Digitale identiteit

We doen steeds meer digitaal, met als gevolg dat ons account steeds meer mogelijkheden biedt. Denk maar eens aan facturen goedkeuren, verlofdagen aanvragen, reisdeclaraties indienen, drukwerk bestellen of het wijzigen van de bankrekening, waarop het salaris wordt gestort.

Deze digitale wereld biedt veel voordelen zoals de mogelijkheid om plaats- en tijdonafhankelijk te werken, en het maakt ons veel minder afhankelijk van anderen om onze zaken te regelen. De digitalisering leidt vaak tot betere stroomlijning van de werkprocessen en tot een - soms drastische - verkorting van de doorlooptijd.

Doordat we steeds meer kunnen doen met ons account, nemen de gevolgen van eventueel misbruik ook toe. Iemand die uw inloggegevens kent, kan in de digitale wereld uw identiteit overnemen. Bedenk eens wat iemand daarmee kan doen, bijvoorbeeld facturen goedkeuren, de bankrekening voor het salaris wijzigen, uw bestanden inzien en uit uw naam e-mail versturen. De risico's hiervan zijn groot. Om die reden stelt de universiteit als eis zorgvuldig met de inloggegevens om te gaan en is het bijvoorbeeld niet toegestaan uw wachtwoord met anderen te delen.

Brute force attack

Wanneer iemand naar uw wachtwoord vraagt, wees dan op uw hoede: ICT-medewerkers zullen nooit om uw wachtwoord vragen. Deel ook op uw eigen afdeling geen wachtwoorden. Soms lijkt het wel gemakkelijk om een collega even toegang tot uw account te geven door het delen van het wachtwoord. Wat ook de reden is, hiervoor is altijd een betere oplossing, raadpleeg de CIT-Servicedesk.

Om te voorkomen dat kwaadwillenden uw wachtwoord kunnen raden, stelt de RUG eisen aan de complexiteit van het wachtwoord. Zoals een minimale lengte en het gebruik van een mix van cijfers, kleine letters en hoofdletters.

Wanneer de gebruikte wachtwoorden voldoende complex en voldoende lengte hebben, dan heeft het uitproberen van lange reeksen wachtwoorden (een zogenoemde 'brute force attack') weinig kans van slagen. Kwaadwillenden gaan om die reden steeds vaker over tot het verzenden van phisingmail.

Legitieme inlogpagina

De verzender van phisingmail heeft als doel de usernaam en wachtwoordcombinatie te achterhalen. Men maakt een inlogpagina die er uit ziet als een legitieme inlogpagina, en probeert via een linkje in de mail u zover te krijgen dat u deze pagina opent en daarop inlogt. Meestal gebeurt dit in bulk, dat wil zeggen dat een grotere groep gebruikers zo'n mailtje krijgt. Soms wordt een veel kleinere groep gebruikers of zelfs een individuele gebruiker geselecteerd, op deze manier kan een meer gerichte aanval worden uitgevoerd en blijft de aanvaller ook makkelijker 'onder de radar'.

Wanneer u vermoedt dat iemand uw wachtwoord kent, wijzig deze dan zo snel mogelijk en informeer direct de Servicedesk, de demand manager of de security manager. Dat geldt ook wanneer u achteraf bedenkt dat u wellicht het slachtoffer bent van een phisingmail-aanval en u helaas uw wachtwoord heeft ingevoerd.

Wanneer u uw wachtwoord wijzigt, let er dan op dat het niet te veel op uw oude wachtwoord lijkt en kies een wachtwoord dat langer is dan de minimale eis.

Windowstoets-L

De meest eenvoudige manier om iemands digitale identiteit over te nemen, is om snel even achter de pc te gaan zitten wanneer de betrokkene even van zijn of haar plaats is. Zorg daarom altijd dat wanneer u uw werkplek verlaat, uw computer gelocked is. Dit kan het makkelijkst door het instellen van een screensaver (met inlogscherm bij reactiveren) of door, op een windowsmachine, het intypen van 'Windowstoets-L'.. Let er ook op, dat geen vertrouwelijke gegevens op het scherm te zien zijn, wanneer u van uw werkplek wegloopt.