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

Phishingmail

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.

Net als vele andere organisaties heeft de universiteit regelmatig te maken met phishingmail-aanvallen. De aanvallende partij probeert daarbij inloggegevens te bemachtigen, door mensen zover te krijgen dat zij naar een nagemaakte inlogpagina gaan en daar hun gebruikersnaam en wachtwoord invullen. Doordat niet iedereen doorheeft dat het om een nagemaakte inlogpagina gaat, bestaat het risico dat zo RUG-inloggegevens in handen van kwaadwillenden komen.

Phishingmailtjes worden steeds knapper gemaakt waardoor het moeilijker wordt ze te herkennen. Nog niet zo lang geleden waren de meeste phishingmails in gebroken Nederlands opgesteld, op het lachwekkende af soms, maar we zien dat het taalgebruik steeds beter wordt. Ook wordt de huisstijl steeds beter nagebootst, zowel in de phishingmail als op de nagemaakte inlogpagina's, die er soms bedrieglijk echt uitzien.

Meehelpen

Wanneer Google bij het afhandelen van binnenkomende mail herkent dat het om dubieuze mail gaat, dan neemt deze tegenmaatregelen, zoals het in de spamfolder plaatsen van de mail. Bij ontvangst van dubieuze mailtjes zoals phishingmail en spam die niet in de spamfolder terecht zijn gekomen, is het van belang deze te markeren als spam. Hiermee helpt u andere mensen en draagt u bij aan een betere geautomatiseerde herkenning in de toekomst.

Ook de RUG zelf neemt maatregelen om de risico's en de impact van phishingmail te beperken. Zodra phishingmail gezien wordt, wordt bijvoorbeeld de verbinding van het RUG-netwerk naar de externe nagemaakte inlogpagina verbroken. Daarmee worden de mensen die binnen de gebouwen van de RUG aan het werk zijn, beschermd. Helaas helpt deze bescherming niet wanneer het mailtje buiten het RUG-netwerk wordt geopend, bijvoorbeeld thuis, onderweg of op een externe werklocatie. Dan komt u wel terecht bij de door de kwaadwillende nagemaakte inlogpagina. Verder werkt de RUG aan de invoering van 'two factor authentication', wat extra bescherming biedt.

Goed opletten

Het blijft dus zaak, goed op te letten bij het lezen van de mail, en linkjes in mailtjes met een gezonde dosis wantrouwen te bekijken. Wees bij het inloggen altijd op de hoede. Controleer of in de adresbalk van de webbrowser een groen slotje staat, en in het adres in de balk inderdaad het domein 'rug.nl' genoemd wordt.

Heeft u twijfel of vermoedt u dat u mogelijk toch via een nagemaakte inlogpagina uw inloggegevens in verkeerde handen heeft gegeven, wijzig dan zo snel mogelijk uw wachtwoord en breng de CIT Servicedesk op de hoogte. Het wijzigen van uw wachtwoord doet u via MyUniversity, kijk onder 'Do It Yourself' en dan bij 'ICT'.

Overigens is phishingmail niet het enige gevaar dat in e-mail schuilt. Het is relatief eenvoudig om een e-mail te versturen met een gefingeerde afzender. Zo kan het gebeuren dat u een e-mailbericht ontvangt dat van een goede bekende lijkt te komen, maar in werkelijkheid door een bedrieger verstuurd is. Wees in ieder geval bij mailtjes waarin verzocht wordt geld over te maken, of die als bijlage een factuur bevatten, daarom altijd op uw hoede. Vertrouwt u het niet, neem dan contact op met de CIT Servicedesk.

Verkeerde ontvanger

Een ongeluk zit in een klein hoekje, dat geldt ook voor de omgang met e-mail. Zo kan het gebeuren dat u bij het verzenden van een e-mail per ongeluk de verkeerde ontvanger heeft gekozen waardoor de e-mail naar het verkeerde adres gaat. Het kan geen kwaad er een gewoonte van te maken, vóór u op de verzendknop drukt, nog even te checken of de geadresseerden inderdaad juist zijn. Nog vervelender is het wanneer een verkeerd geadresseerde e-mail persoonsgegevens bevat. De Autoriteit Persoonsgegevens beschouwt e-mails die persoonsgegevens bevatten en naar de verkeerde ontvanger zijn verstuurt, als datalek. Mocht u dat overkomen, meldt dit dan bij het meldpunt voor datalekken bij de RUG: **cert@security.rug.nl**.