Blijf alert op phishing-mail!

Geplaatst op 12 apr 2023 door

Op 25 maart 2023 maakt onderzoeksbureau <> bekend dat persoonsgegevens gestolen zijn als gevolg van een datalek bij een softwareleverancier. Omdat organisaties als <><><> (indirect) gebruik maken van deze software, zijn persoonsgegevens van miljoenen mensen buitgemaakt door criminelen.

Ook medewerkers van de OU kunnen privé of zakelijk geraakt worden door deze hack. De persoonsgegevens die werden ingezien en/of werden gestolen kunnen mogelijk worden gebruikt om een phishing aanval uit te voeren. Wij vragen je daarom extra alert te zijn op zogenaamde phishing-berichten. Phishing e-mails lijken van bekende en vertrouwde afzenders af te komen (bv. van Microsoft, een familielid of een collega). Deze e-mails hengelen ofwel rechtstreeks naar het wachtwoord of bankgegevens, of bevatten een bijlage in de vorm van een Word-document (doc(x)-bestand), een gezipped bestand of een link naar een Word-document. Bij het openen van zo'n bijlage kunnen er kwaadwillende macro's actief worden waardoor malafide programmatuur lokaal op de werkplek wordt geïnstalleerd. De kans bestaat dan ook dat de malware op dat moment probeert de bestanden op de werkplek en andere systemen in het netwerk te infecteren. Ook meldden we eerder dat phishing plaatsvindt met behulp van QR-codes.

Wij benadrukken daarom met klem:

- Mocht je een vreemde e-mail ontvangen met daarin een niet vertrouwde inhoud, reageer daar dan niet op;
- Heb je de mail geopend, klik dan nooit op de bijlage of de link in het bericht;
- Open je onverhoopt toch een dergelijke bijlage en wordt er gevraagd om macro's toe te staan, doe dit dan niet, breek het 'proces' af en sluit de e-mail;
- Geef ook nooit wachtwoorden of bankgegevens af;
- Ontvang je een mail met een bijlage waarover je twijfelt, want de mail is wel bijvoorbeeld van een voor jou bekende afzender en je verwacht een mail met bijlage, neem dan contact op met de Servicedesk. De Servicedesk kan helpen beoordelen of een bijlage te vertrouwen is.

Mocht je vermoeden dat je toch op een link geklikt hebt óf heb je toch een bijlage geopend, waarschuw dan onmiddellijk de Servicedesk, servicedesk@ou.nl (telefonisch 045-5762306).

Remain on the lookout for phishing emails!

On March 25, 2023 research agency <> announced that personal data had been stolen because of a data breach at a software supplier. Because organizations such as <><><><> (indirectly) use this software, personal data of millions of people have been captured by criminals.

Employees of the OU can also be affected privately or professionally by this hack. The personal data that was accessed and/or stolen may possibly be used to carry out a phishing attack. We therefore ask you to be extra vigilant to so-called phishing emails. Phishing emails seem to come from known and trusted senders (for example, Microsoft, a family member, or a colleague). These emails either directly fish for your password or bank details or contain an attachment in the form of a Word document (doc (x) file), a zipped file, or a link to a Word document. When opening such an attachment, malicious macros can become active, causing malicious software to be installed locally on the computer. There is therefore a chance that the malware will try to infect the files on the computer and other systems in the network at that time. We also reported earlier on the intranet that phishing takes place using QR codes.

We therefore emphasize:

- If you receive a strange e-mail containing unfamiliar content, do not respond to it.
- Once you have opened the mail, never click on the attachment or the link in the message.
- If you unexpectedly open such an attachment and are asked to allow macros, do not do this, stop the "process" and close the e-mail.
- Never provide passwords or bank details.
- If you receive an e-mail with an attachment that you are unsure about, because the e-mail is, for example, from a sender known to you and you expect an e-mail with an attachment, please contact the ServiceDesk. The ServiceDesk can help assess whether an attachment can be trusted.

If you suspect that you have nevertheless clicked on a link or if you have nevertheless opened an attachment, immediately notify the Servicedesk, servicedesk@ou.nl (by telephone 045-5762306).

You can also contact the ServiceDesk for additional questions.

Trefwoorden: Nieuws-Ict

RELEVANTE APPLICATIES

Nieuws mijnOU
Overzicht van alle interne nieuwsberichten.

Nieuws www.ou.nl
Overzicht van alle externe nieuwsberichten.

Organisatie

Overzicht van alle gremia, faculteiten en afdelingen.

Secretariaten
Overzicht van de contactgegevens van de secretariaten.

Studiecentra
Overzicht van de studiecentra, met sluipnummers

Servicedesk
Eerste aanspreekpunt voor facilitaire en ict-vragen.

MEDEWERKERS

Zoek medewerkers