Tekst Jolein de Rooij

Uitsmijter

Pas op voor phishing op maat!

Tijdens zijn promotieonderzoek slaagde Pavlo Burda van de Technische Universiteit Eindhoven erin om verontrustend veel mensen in zijn phishingmail te laten trappen.

FOTO: VINCENT VAN DEN HOOGEN

Wie: Pavlo Burda
Waar: Eindhoven
Wat: phishing
Waarom: bestrijden

In de toekomst wordt phishing nog overtuigender, zegt onderzoeker Pavlo Burda van de Technische Universiteit Eindhoven (TU/e). Dat komt omdat deze vorm van oplichting steeds persoonlijker gaat worden. Hoe kun je je daartegen wapenen?

Hoe gevaarlijk is phishing?

"Bij phishing probeert een crimineel iemand iets doms te laten doen, zoals het delen van identiteits- of inloggegevens, of het installeren van malware. Dat kan het startpunt zijn voor een heel scala aan aanvalstechnieken. Die worden niet alleen uitgevoerd door criminelen; ook bedrijven proberen zo concurrenten te bespioneren of te saboteren. En staten zetten phishing in voor elektronische oorlogsvoering, om in buitenlandse computersystemen binnen te dringen."

Waarom zijn we er vatbaar voor?

"Dat komt door de manier waarop onze hersens werken. We kunnen goed systematisch nadenken en op een rationele manier beslissingen nemen, maar dat kost best veel energie. Ons brein houdt dat niet de hele dag vol. Bovendien gaat het traag. Daarom verrichten we veel handelingen op de automatische piloot. Als je bijvoorbeeld aan het autorijden bent en het licht springt op groen, trek je vrijwel gedachteloos op. Helaas kunnen oplichters ook misbruik maken van onze automatische piloot."

Hoe maken ze daar misbruik van?

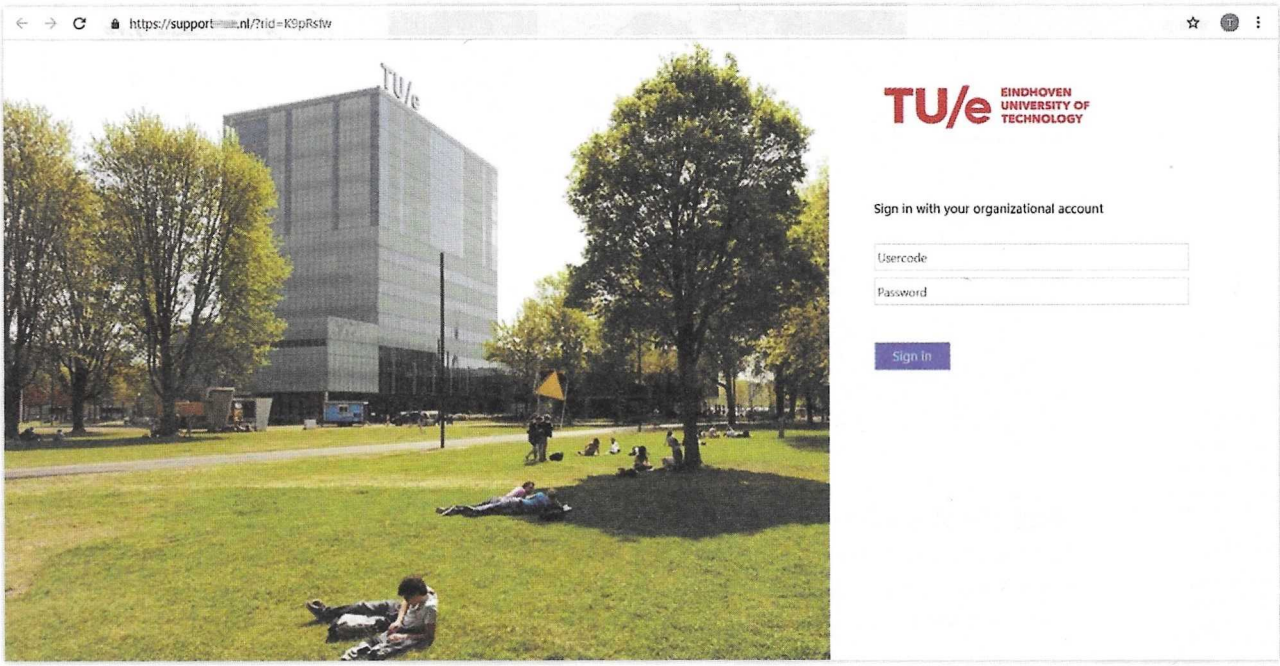
"De Amerikaanse psycholoog Robert Cialdini heeft daar veel over geschreven. Zo zijn we bijzonder gevoelig voor autoriteit. We zijn daarom alert op allerlei signalen die daarop wijzen; van het uniform van een politieagent, tot de diploma's aan de muur bij een arts. Ook hechten we aan wederkerigheid: als iemand iets voor ons doet, doen we graag iets terug. Dat is precies de reden dat je in restaurants gratis snoepjes bij de rekening krijgt. Dan geef je meer en eerder fooi. Ook zijn we gevoelig voor schaarste en tijdsdruk. Op Black Friday spelen bedrijven daarop in; het gevoel dat je iets mist als je niet snel toeslaat. Zo zijn er allerlei trucjes waarmee je mensen kunt overhalen iets te doen wat ze eigenlijk niet van plan waren. Die trucjes zijn er allemaal op gericht ons gezonde verstand uit te schakelen, en ons te laten overschakelen op de automatische piloot."

Criminelen schakelen onze ratio uit?

"Ja, bijvoorbeeld met een mix van tijdsdruk en autoriteitsdreiging. Dan krijgt een boekhouder bijvoorbeeld op vrijdagmiddag zogenaamd een mail van de directeur, die hem maant om een factuur nog voor het weekend te betalen. Een ander voorbeeld: mensen zijn er inmiddels aan gewend geraakt dat ze kunnen betalen door een QR-code te scannen. Van die gewenning maakten criminelen in de VS een paar maanden geleden misbruik op een parkeerplaats. Ze plakten een sticker op de parkeerzuil, precies over de bestaande QR-code heen. Zo lieten ze nietsvermoedende parkeerders geld overmaken naar hun eigen bankrekening. Tijdens mijn promotieonderzoek heb ik dit soort mechanismen zo exact mogelijk in kaart gebracht, ook om te kunnen verklaren waarom de ene aanval succesvoller is dan de andere."

Hoe heb je dat onderzocht?

"Onze onderzoeksgroep heeft onder meer een phishing-experiment gedaan. We hebben in totaal zo'n 750 mensen een



In de phishing-experimenten die Pavlo deed, lokte hij mensen naar een nepsite waar ze hun inlognaam en wachtwoord moesten invullen. In het echt maakt de TU/e overigens al een paar jaar gebruik van multifactor-authenticatie.

phishingmail gestuurd, deels bij de TU/e en deels bij een groot Nederlands adviesbureau. Die laatste organisatie bleek gevoeliger voor phishing dan mijn oude universiteit: dertig procent van de bedrijfswerknemers . vulde zijn of haar inlognaam en wachtwoord in op een nepsite, tegenover tien procent van de universiteitsmedewerkers. Ook waren juniormedewerkers gevoeliger voor phishingmails die afkomstig leken van iemand met autoriteit binnen hun organisatie. Bij het adviesbureau trapte 52 procent van hen er zelfs in. Maar nog meer van invloed bleek in hoeverre de mail persoonlijk was gemaakt. Werd iemand met zijn of haar eigen naam aangesproken? Ging het over een thema dat al bij die persoon bekend was? Werd de mail zogenaamd verstuurd door iemand van de organisatie?"

Is phishing op maat extra gevaarlijk?

"Ja, en dat is slecht nieuws. In de toekomst gaan we er namelijk waarschijnlijk veel meer van ontvangen. Dat komt omdat mensen veel gegevens over zichzelf prijsgeven op sociale media. Ook komen er regelmatig databases met persoonsgegevens op straat te liggen. Door al die data te combineren, kun je behoorlijk gedetailleerde persoonsprofielen opstellen. Daarmee kun je phishing op maat maken, ook geautomatiseerd. Kunstmatige intelligentie biedt daarvoor nog eens extra mogelijkheden. Zo las ik over een 56-jarige vrouw uit Enschede die vorig jaar dacht te worden gebeld door haar zoon. Hij was in paniek en vertelde zojuist een dodelijk ongeval te hebben veroorzaakt. Alleen als hij of zijn moeder de uitvaartkosten vergoedde, zou hij niet worden aangehouden. De moeder was overstuur en overal toe bereid, totdat haar zoon plotseling de kamer inliep. Toen besefte ze dat het telefoontje nep was. De afpersers hadden de stem van haar zoon gekloond."

Hoe kunnen we ons wapenen?

"Eigenlijk niet. We zijn allemaal gevoelig voor phishing, ook jij en ik. Je kunt het wel moeilijker maken om misbruik te maken van gestolen inloggegevens door het instellen van multifactorauthenticatie. Bij phishing-aanvallen is daarnaast rapporteren belangrijk. Zo bleek in een van mijn experimenten dat sommige mensen phishing onmiddellijk doorhadden, en daarvan ook meteen melding deden bij hun ICT-afdeling. Die mensen moet je koesteren. En je moet het als organisatie makkelijk maken om phishing te rapporteren. Daarna moet je snel reageren, want elk uur neemt de schade toe. In mijn onderzoek bleek dat na vier uur al driekwart van de slachtoffers was gevallen."

Welke adviezen heb je voor de lezers?

"Profielen op sociale netwerken als Facebook, Instagram en LinkedIn kun je beter niet publiek toegankelijk maken, want er zijn software-robots die het gehele internet afstruinen op zoek naar data. En als je twijfelt over een berichtje, reageer dan niet vanaf je telefoon. Wacht als het even kan tot je weer thuis bent en rustig achter je computer zit. Dan heb je ook meer tijd gehad om over het bericht na te denken. Smartphones zijn erg gebruiksvriendelijk, maar op een groot scherm zie je veel meer details. Dat verhoogt de kans dat je phishing herkent."

Oproep

Doe je iets bijzonders met jouw computer? Of heb je een handige softwareoplossing voor je hobby bedacht? Stuur dan een e-mail met als onderwerp 'Rubriek Uitsmijter' naar redactie@computeridee.nl
Wie weet kom je ermee in Computer Idee.

Sites

- www.pavlo.it
- www.kwikr.nl/nieuwetruc
- www.kwikr.nl/qrscam
- www.kwikr.nl/weaklink