



WAT IS PHISHING?

Phishing is een vorm van oplichting via internet. Door een e-mail probeert een oplichter (phisher) uw persoonlijke gegevens als creditcardnummer, bankgegevens, pincode of identiteitsgegevens te achterhalen. Deze e-mail lijkt afkomstig te zijn van een betrouwbare instantie, zoals uw creditcardmaatschappij of bank. Met deze gegevens kan de oplichter vervolgens bijvoorbeeld geld van uw rekening halen of andere producten/diensten op uw naam aanschaffen.



WAT IS CRYPTOWARE?

Bij een Cryptoware-infectie, veroorzaakt door bijvoorbeeld te klikken op een kwaadaardige e-mail, worden bestanden op de computer versleuteld. Vervolgens wordt er door cybercriminelen veelal losgeld gevraagd voor de ontsleutelingscode. Tot die tijd zijn de computer, of bestanden daarop, niet meer toegankelijk.



HOE HERKENT U PHISHING?

Het is vaak moeilijk een phishing e-mail te onderscheiden van een authentieke e-mail. Toch is er een aantal kenmerken te noemen waaraan u een phishing e-mail kunt herkennen.

- Gerenommeerde banken, creditcardmaatschappijen en andere legitieme bedrijven vragen u nooit per e-mail om persoonlijke gegevens zoals creditcardnummer of wachtwoorden.
- Phishing e-mails spelen vaak in op uw angst opgelicht te worden, uw account kwijt te raken of op een andere dringende redenen om zo snel mogelijk te reageren.
- Een phishing e-mail is meestal onpersoonlijk: de aanhef luidt bijvoorbeeld "Beste klant". Maar let op: ook gepersonaliseerde e-mail kan nog steeds nep zijn!

HOE HERKEN JE CRYPTOWARE?

Cryptoware wordt vaak verstuurd als een ZIP-bestand. Dit soort bestanden zijn veelal niet goed te scannen door een virusscanner. Daarbij worden dit soort bestanden veel verzonden "namens" bekende bedrijven zoals de Wehkamp, PostNL, Belastingdienst etc. Dergelijke bedrijven zullen u nooit per e-mail een ZIP-bestand toesturen als u daar niet vooraf van op de hoogte bent (Dit gebeurt eigenlijk alleen als u reeds persoonlijk contact heeft met iemand). In dit soort e-mailberichten is vaak te lezen dat u iets heeft gewonnen, u nog iets moet betalen of een ander bericht waardoor u perse zou willen weten wat er in het ZIP-bestand staat. Soms zijn de e-mailberichten ook te herkennen aan een slechte vertaling. Hierdoor zijn ze niet in goed Nederlands geschreven. Toch lijken ze erg veel op standaardberichten van bekende bedrijven.

HOE VOORKOM IK MISBRUIK / BESMETTING?

Naast een goede virusscanner is het erg belangrijk dat mensen bekend zijn met de nieuwe phishing-/cryptoware-methodes. Door de organisatie hiermee bekend te maken let men sneller op de herkenningpunten van berichten. Een virusscanner kan helaas dit soort berichten niet altijd blokkeren. Het is daarom belangrijk dat berichten uit een onherkenbare bron niet direct gezien wordt als "veilig" en niet direct alle bijlages zomaar geopend worden. Indien er getwijfeld wordt over dergelijke berichten kunt u het beste overleggen met een collega of met uw ICT-contactpersoon.

MEER INFORMATIE?

www.utahconsulting.nl
www.fraudehelpdesk.nl