2. Opgelet voor phishing

1. HOE HERKEN IK EEN PHISHING E-MAIL?

1. Verdacht afzenderadres

   - Controleer het domein: Phishing-e-mails komen vaak van adressen die lijken op legitieme adressen maar kleine variaties hebben, zoals "support@paypa1.com" in plaats van "support@paypal.com".
   - Onverwachte afzenders: Als je een e-mail ontvangt van een afzender die je niet herkent, wees dan voorzichtig.

2. Algemene begroetingen en taal

   - Gebrek aan personalisatie: Phishing e-mails gebruiken vaak algemene begroetingen zoals "Beste klant" of "Beste gebruiker" in plaats van je naam. Ze kunnen echter ook persoonlijk zijn!
   - Slechte grammatica en spelling: Veel phishing e-mails bevatten spelfouten, grammaticale fouten of onhandige formuleringen.

3. Urgentie en bedreigingen

   - Onmiddellijke actie vereist: E-mails die een gevoel van urgentie oproepen, zoals beweren dat uw account zal worden geschorst tenzij u onmiddellijk actie onderneemt, zijn vaak phishing-pogingen.
   - Afschriktactieken: Dreigen met negatieve gevolgen als je niet snel reageert is een rode vlag.

4. Ongebruikelijke verzoeken

   - Gevoelige informatie: Legitieme bedrijven zullen nooit via e-mail om gevoelige informatie vragen (zoals wachtwoorden, creditcardnummers of sofinummers).
   - Onverwachte bijlagen of koppelingen: Wees op je hoede voor e-mails met ongevraagde bijlagen of links, vooral als ze beweren belangrijke documenten of updates te zijn.

5. Inconsistenties in de inhoud van e-mails

   - Niet overeenkomende URL's: Beweeg met de muis over links om de werkelijke URL te zien. Als de linktekst het ene zegt, maar de URL ergens anders naartoe wijst, is het waarschijnlijk een phishing-poging.
   - Inconsistente huisstijl: Let op inconsistenties in logo's, kleuren of e-mailindeling in vergelijking met eerdere legitieme e-mails van dezelfde afzender.

6. Gespoofde websites

   - Lookalike websites: Phishing-e-mails leiden u vaak naar websites die er bijna identiek uitzien als legitieme sites. Controleer de URL zorgvuldig op spelfouten of ongebruikelijke domeinen.
   - Niet-beveiligde websites: Legitieme sites maken meestal gebruik van HTTPS. Als de site waar je naartoe wordt geleid geen HTTPS heeft (zoek naar het hangslotsymbool in de adresbalk), is dat een waarschuwingsteken.

7. Onverwachte bijlagen

   - Vermijd openen: Open geen bijlagen die je niet verwacht. Deze kunnen malware of ransomware bevatten.
   - Ongebruikelijke bestandstypen: Wees vooral voorzichtig met bijlagen met ongebruikelijke bestandstypen (.exe, .scr, .zip).

8. Ongebruikelijke toon of stijl

   - Niet gebruikelijk: Als de toon of stijl van de e-mail niet overeenkomt met wat je verwacht van de afzender, kan het een phishing-poging zijn. Als bijvoorbeeld een collega die meestal formeel schrijft opeens een heel informele e-mail stuurt, is dat verdacht.

9. E-mailadres en weergavenaam komen niet overeen

   - Kijk goed: De weergavenaam kan er correct uitzien, maar het echte e-mailadres kan anders zijn. Controleer altijd het volledige e-mailadres.

10. Gebruik van openbare e-maildomeinen

- Openbare domeinen: Wees op uw hoede voor e-mails van zogenaamd gerenommeerde bedrijven die openbare e-maildomeinen zoals Gmail, Yahoo of Hotmail gebruiken in plaats van hun officiële bedrijfsdomein.

2. VERIFIEER VERDACHTE E-MAILS

1. Neem rechtstreeks contact op met de afzender

- Als een e-mail er verdacht uitziet, maar afkomstig lijkt te zijn van iemand die je kent of een bedrijf waarmee je zaken doet, neem dan rechtstreeks contact op via een bekend telefoonnummer of e-mailadres (niet door te antwoorden op de verdachte e-mail).

2. Controleer officiële kanalen

- Controleer de informatie via de officiële websites van het bedrijf of de kanalen van de klantenservice.

3. Gebruik anti-phishing programma's

- Gebruik e-mail filter en anti-phishing tools van uw e-mail service provider of cyberbeveiligingssoftware.

3. SAMENGEVAT

Door waakzaam te blijven en op deze veelvoorkomende tekenen van phishing e-mails te letten, kan je jezelf en het bedrijf beschermen tegen deze zwendelpraktijken. Controleer altijd dubbel voordat je op links klikt, bijlagen downloadt of persoonlijke informatie verstrekt in antwoord op een e-mail.

4. MEER OVER PHISHING

Phishing: the most common attack - Knowledge Base - Intersoft Electronics (inventive-engineering.com)

Samen houden we Intersoft Electronics cyber secure

INTERSOFT ELECTRONICS NV
Lammerdries-Oost 27 | B-2250 Olen | Belgium
Tel +32 14 23 18 11 | support@intersoft-electronics.com