Allmän information om nätfiske

Termen nätfiske beskriver ett försök att lura människor i illegalt syfte. Ibland vill nätfiskarna installera skadlig kod på personens dator och andra gånger uppmanar de människor att lämna ifrån sig känslig information. Nätfiskemeddelanden kan skickas via e-post, SMS eller sociala nätverk.

Bedragare använder informationen som människor lämnar ifrån sig för att gynna sig själva, installera skadlig kod för att ta kontroll över datasystem eller stjäla värdefull information. Bedragare skickar miljoner av nätfiskemeddelanden till en minimal kostnad. Många av dessa meddelanden lockar mottagare att klicka på en skadlig länk, vanligtvis maskerad till en legitim länk från ett företag eller en ofarlig webbsida.

Kunskap om hur webbadresser (URL:er) är uppbyggda kan bidra till att upptäcka nätfiskemeddelanden. Avsändare, utseende och innehåll kan man ignorera eftersom detta är lätt att förfalska. Den viktigaste regeln för mottagare är att kontrollera alla länkar innan man klickar på dem. Här vill vi förklara hur man kontrollerar huruvida en länk är legitim eller inte.

Råd

Innehållet i denna folder behandlar en av de vanligaste typerna av nätfiske. Fokus är att upptäcka maskerade webbadresser (URL:er) som används för nätfiske.

Hitta mer information och appen NoPhish
https://www.secuso.org/nophish

Kontakt

Datavetenskap vid
Karlstads universitet

Karlstads universitet
Institutionen för matematik
och datavetenskap
651 88 Karlstad, Sverige
E-post: cs@kau.se

https://www.kau.se/cs

NoPhish

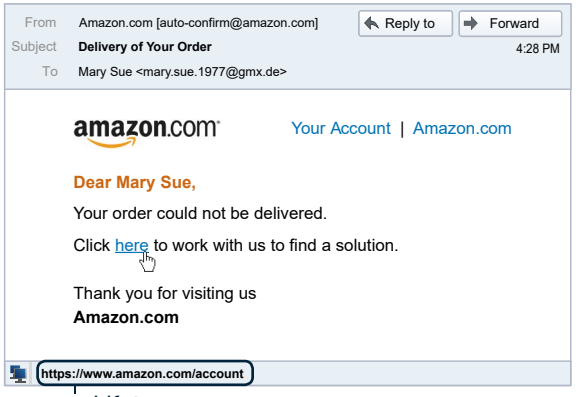
Guide för att upptäcka nätfiske

SECURITY · USABILITY · SOCIETY

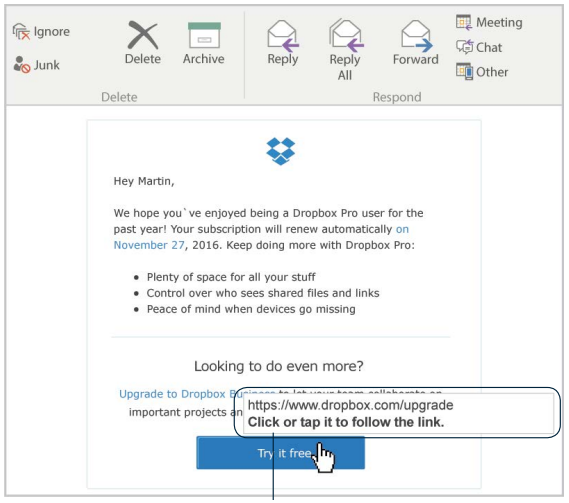
TECHNISCHE UNIVERSITÄT DARMSTADT

Följande riktlinjer hjälper dig avgöra legitimiteten hos en webbadress:

1.) För att hitta det verkliga målet för en klickbar länk (URL:en) håll muspekaren över länken utan att klicka på den. Den riktiga mållänken (URL:en) visas antingen i ett litet popup-fönster bredvid länken eller i websidans/meddelandets sidfot.



sidfot



popup-fönster

Hur man upptäcker den verkliga destinationen för en länk på mobila enheter (t.ex. smartphone eller tablett), beror på enheten som används. Vanligtvis kan man trycka lätt på en länk under 2 sekunder utan att klicka på den, då öppnas en dialogruta där den faktiska destinationen visas.

Dialogruta

2.) Var uppmärksam på den så kallade "vem-delen" när du kontrollerar webbadressen.

https://www.facebook.com/login/

Vem-delen (företag.plats)

"Vem-delen" är helt enkelt de två sista orden innan det första ensamma snedstrecket / (i det här fallet facebook.com) i en webbadress. "Vem-delen" är den viktigaste delen för att upptäcka nätfiske genom falska webbadresser. Den tekniska termen för "vem-delen" är domän.

3.) Om utrymmet mellan "http://" och det tredje snedstrecket är numeriskt är det en stark indikation på att det är en skadlig domän. Bäst att ta det säkra för det osäkra och inte klicka på en sådan länk.

✗ https://95.130.22.98/google.com.secure-login.com/
✓ https://mail.google.com/intl/com/mail/help/about.html/

4.) I en del meddelanden placeras det riktiga företagsnamnet någon annanstans i webbadressen än i vem-delen, för att minska misstänksamheten. Bäst att låta bli att klicka även på dessa länkar.

✗ https://www.amazon.com.online-shopping.com/
✗ http://online-shopping.com/https://www.amazon.com
✓ https://www.amazon.com/online-shopping

5.) Undersök noga om vem-delen har stavfel (till exempel zz istället för z; eller kc istället för ck). Om du hittar liknande stavfel så lita inte på länken eller webbsidan och lämna inte ut några personuppgifter!

✗ https://www.amazzon.com
✓ https://www.amazon.com
✗ https://www.blokket.se
✓ https://www.blocket.se

6.) Undersök vem-delen noggrant för att upptäcka användning av bokstäver eller siffror som liknar varandra (till exempel "rn" istället "m" eller "1" istället för "l"). Om vem-delen har bokstäver som är utbytta mot liknande bokstäver eller siffror, lämna inte heller här ut några personuppgfter!

✗ https://www.arnazon.com
✓ https://www.amazon.com
✗ www.hernnet.se
✓ www.hemnet.se

7.) Ibland görs förändringar i den äkta "vem-delen" (t ex: facebook-secure). Detta är en stark indikation på försök till nätfiske. De här attackerna är svåra att upptäcka eftersom du måste veta hur vem-delen borde se ut. En annan svårighet är att vissa legitima webbsidor inte har en tydlig vem-del. Om du är osäker så använd en sökmotor för att hitta företagets äkta URL.

✗ https://www.facebook-secured.com/
✓ https://www.facebook.com/

8.) Lämna bara ut känslig data (som lösenord och kontoinformation) om URLen startar med https://

✗ http://internetbanken.privat.nordea.se/nsp/login
✓ https://internetbanken.privat.nordea.se/nsp/login

Notera att de här reglerna är skapade i ett svensk kontext. En del länder använder en kombination, liknande ett dubbelefternamn istället för .com. Storbritannien t ex använder .co.uk eller org.uk. I det fallet räknas de tre sista orden innan det första enkla snedstrecket, som vem-delen.