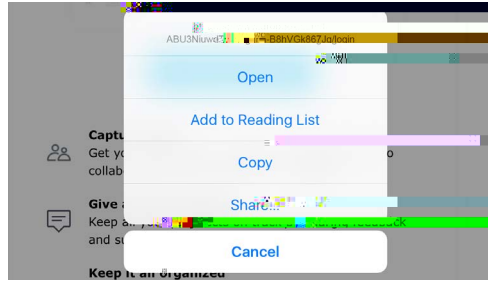


NoPhish





6.) Undersök vem-delen noggrant för att upptäcka användning av bokstäver eller siffror som liknar varandra (till exempel "rn" istället för "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 personuppgifter!

<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 svenskt kontext. En del länder använder en kombination, liknande