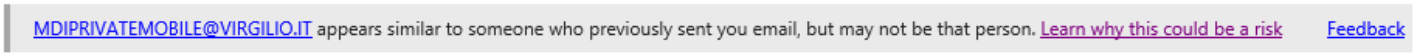
Anti-Phishing Policy - Security Banner

Översikt

Det här verktyget ska informera användare om möjliga bedrägerier via e-post som många studenter och personal vid högskolan får varje vecka.

- Policyn jämför inkommande e-postmeddelanden med historiken i din inkorg
- När samma **namn** på meddelandet matchar ett **namn** i din e-posthistorik, men **adressen** skiljer sig från den tidigare **adressen**, flaggar anti-phishing policyn meddelandet som farligt och lägger till en banner längst upp för att varna dig för skillnaden



- Var försiktig med e-post som har en banner som den ovan.
- Om meddelandet verkar komma från din chef eller medarbetare, bekräfta meddelandet genom att ringa ett känt nummer eller genom att skicka ett separat meddelande till deras högskoleadress. (Använd inte något nummer eller adress som finns i det flaggade meddelandet)

Fördelar

Kommer anti-phishing policy flagga en riktig adress som misstänkt?

- Ja - ibland. Det händer att man av misstag skickar ett legitimt meddelande från sitt personliga konto istället för sitt högskolekonto.
- Detta händer oftast när avsändaren använder sin mobil för att skicka meddelandet då e-postappen ofta är konfigurerad att skicka e-post från både en privat adress och högskoleadressen.

Hur kan jag förhindra att legitima meddelanden jag skickar flaggas med en säkerhetsbanner?

- Det bästa sättet att förhindra att dina meddelanden flaggas är att ***alltid*** använda din högskoleadress för att skicka meddelanden till kollegor och studenter på JU.
- Använd **Outlook Mobile**-appen för att hantera din högskoleadress och den inbyggda e-postappen för att hantera din privata e-post. Att använda olika e-postappar för arbets- och privat e-post är det bästa rådet.

Metoder

Många av högskolans anställda råkar varje vecka ut för enkla bedrägerier som kan lura dig personligen på flera tusen kronor eller tusentals av JU:s medel. Det är väldigt enkelt och därför också väldigt effektivt. Angriparen använder högskolans webbsida för att hitta listor på personer som rapporterar till exempelvis rektor eller en chef.

Angriparen skapar en legitim e-postadress med chefens namn, till exempel MDIPRIVATEMOBILE@VIRGILIO.IT.
Angriparen skickar sedan ett enkelt meddelande:

From: Dean Deansson <MDIPRIVATEMOBILE@VIRGILIO.IT>

MDIPRIVATEMOBILE@VIRGILIO.IT appears similar to someone who previously sent you email, but may not be that person. Learn why this could be a risk Feedback

Subject: betalning

Hej

Vi behöver skicka en betalning på 17850,00 € till Belgien idag.

Det går att ordna?

vilken information behöver du för att göra denna betalning?

Med vänlig hälsning

Dean Deansson

Dean JU

Angriparen kan också försöka övertyga dig att köpa presentkort och skicka kort på aktiveringskoderna på presentkorten. Den här typen av attack är mest effektiv mot nyanställda.