Ibland dyker det upp e-postmeddelanden där någon ber om hjälp med att skicka pengar, köpa tjänster eller liknande. Denna metod kallas bland annat “Display Name Spoofing” eller ”Impersonations” och de är tyvärr svåra att bli av med helt.

Display Name Spoofing är en taktik som används av hackare för att få ett bedrägligt e-postmeddelande att se legitimt ut. Det vanliga tricket är att utge sig för någon som du personligen känner och ofta utbyter mejl med. Detta kan vara din chef, kollegor, affärspartners, kundvårdsrepresentanter, etc. Målet är att skapa förtroende och få känslig information som bankuppgifter, personnummer, inloggningsuppgifter, viktiga dokument, medicinska rapporter, passuppgifter, etc. De kan till och med lura dig att göra onlinetransaktioner.

Hur fungerar Display Name Spoofing?

Låt oss se på en vanlig teknik för detta. Nätfiskare skapar en ny e-postadress med hjälp av kostnadsfria e-postleverantörer som Gmail, Yahoo, Outlook, etc. Den nya e-postadressen liknar adressen som ska efterliknas och har samma visningsnamn. Den kringgår anti-spam-filter eftersom e-postadressen är tekniskt giltig och oförfalskad.

Det fungerar helt enkelt på det faktum att mottagare ofta inte tittar på e-postadressen, utan istället bara ser visningsnamnet. De ignorerar också att domännamnet saknas och den låtsade avsändarens namn nämns och uppfattar det som avsändarens personliga e-postadress.

Nätfiskare använder också samma e-postsignaturer längst ner i e-postmeddelandena för att få det att se ut som om det kommer från den äkta avsändaren.

Varför är Display Name Spoofing mer framgångsrikt på mobila enheter?

Vet du att spoofing av e-postvisningsnamn är mer framgångsrikt på mobiler? Detta beror på att mobila enheter inte visar metadata; därför ser mottagarna bara visningsnamnet, inte Från:-adressen. Detta gör sådana bedrägerier lättare, avslöjar offer för att dela känsliga

detaljer, klicka på skadliga länkar, göra onlinetransaktioner, etc.

Skärmstorleken på en mobil enhet är mindre än på en bärbar eller stationär dator. Som ett resultat blir mängden information som kan visas betydligt mindre – och e-postklienter på mobila enheter är anpassade för detta. De flesta, om inte alla, e-postklienter på mobila enheter visar inte avsändarens e-postadress, utan visar istället bara visningsnamnet. Detta är en stor fördel för hackare.

Hur klarar e-postmeddelanden med Display Name Spoofing sig förbi skräppostfilter?

Att veta hur man stoppar spoofing av visningsnamn är avgörande eftersom dessa e-postmeddelanden verkar legitima vid tillfällig inspektion av e-postfilter mot skräppost. Detta händer eftersom e-postleverantörer endast visar visningsnamnet över e-postadressen.

E-postmeddelandena passerar filtren eftersom de saknar tvivelaktigt innehåll som oönskade, oönskade eller virusinfekterade länkar. Det är därför anti-spam-filter inte är effektiva mot utgående nätfiskeattacker, spoofingattacker, domänimitation, skadlig programvara och ransomware.

Hur förhindrar man Display Name Spoofing?

Utbilda dig själv och dina anställda för att se de röda flaggorna som indikerar olagliga e-postmeddelanden för att förhindra Display Name Spoofing. Här är några saker som man bör vara försiktig med.

- **Misstänkt avsändaradress:** Förhindra effektivt hackare från att försöka falska e-postattacker i ditt företags namn genom att uppmärksamma e-postadressen, särskilt domännamnet. Korskontrollera även e-postadresser från tidigare utbytta konversationer.
- **Inget SSL-certifikat**: SSL står för Secure Sockets Layer, en kod som säkrar onlinekonversationer. Den innehåller information om domännamn, ägare, associerade underdomäner etc. Så klicka inte på länkar som börjar med “http” istället för “https”. “S” indikerar SSL-skydd.
  Webbplatser utan SSL-certifikat kan förknippas med bedrägliga aktiviteter. Att läsa information på dem är ok, men att fylla i formulär mm på dem bör man undvika.
- **Oprofessionellt innehåll:** Håll utkik efter grammatik- och stavfel, oprofessionell grafik

och dåligt formaterade e-postmeddelanden eftersom hackare inte anlitar specialister för att utföra sådana jobb. De skapar till och med en känsla av brådska i tonen genom att använda ord som “inom en timme, “utan dröjsmål” etc. för att skynda dig igenom innehållet så att du inte upptäcker misstag.

- **Kontrollera länkar innan du klickar:** Håll muspekaren över länken eller hyperlänkad text utan att klicka på den och titta i det nedre vänstra hörnet av skärmen. Du kommer att se hela länken. Klicka för att bara öppna webbsidan om du är säker. Om du av misstag har klickat på en nätfiske-länk, koppla från internet och kör en antivirusskanning.
- **Ovanliga förfrågningar:** Om du har fått en begäran om att dela viktig information som OTP:er, lösenord, personnummer, ekonomiska detaljer etc., finns det en möjlighet att det är en nätfiske-länk. Var speciellt försiktig med länkar som leder dig till inloggningssidor.
- **Utbilda dina teammedlemmar:** Träna dina teammedlemmar i hur man stoppar Display Name Spoofing och andra typer av cyberattacker. Instruera dem om röda flaggor som okänd avsändare, ovanliga förfrågningar, en känsla av brådska i tonen, oönskade bilagor och länkar, etc.

Det finns ytterligare skydd som hjälper till att skydda organisationer, både spam-skydd, antivirus-tjäsnter och inställningar för e-postdomäner så som SPF, DKIM och DMARC. Kontakta oss om du vill veta mer.