Advarsel – der udsendes jævnligt bølger af falske e-mails

Har du fået en mail, der ser ud til at være fra en bank, Skat, Nets, Paypal, MasterCard eller Visa – eller fra en, du aldrig har hørt om før, som lige kan fortælle, at du har vundet en million Euro eller bare skal have lidt skat tilbage?

Så kan du være helt sikker på, at det er en såkaldt 'phishing-mail', der er havnet i din ind-bakke! Muligheden for, at du bliver bedt om at indtaste fortrolige oplysninger er absolut til stede.

Formålet er at lokke fortrolige oplysninger ud af dig – enten som netbank-kunde eller kortholder. Oplysninger, som de kriminelle anvender til at stjæle penge fra dig! De beder for eksempel om dit kontonummer., de sidste fire cifre i dit CPR-nummer, SecureCode, kortnummer, udløbsdato og kortverifikationskode (CVV) fra dig

Du må aldrig afgive dine oplysninger – heller ikke selv om der står, at det kan have ubehagelige konsekvenser for dig, hvis du ikke gør det. Dine oplysninger vil blive misbrugt, hvis du gør.

Disse e-mails er kun tilsyneladende afsendt med ovenstående som afsender og sendes jævnligt til vilkårlige e-mailadresser med forskellige overskrifter.

Ingen myndigheder, banker, Visa og/eller MasterCard kontakter aldrig kunder pr. e-mail for at bede om bekræftelse af kortdata, cpr-numre, adgangskoder eller andre personlige oplysninger.

Man skal derfor aldrig følge opfordringerne, men derimod slette e-mailen med det samme! Slet den helt – også fra papirkurven. Og undlad helst at åbne mailen, men lad altid være med at klikke på eventuelle links og vedhæftede filer i mailen.

Og slet altid mystiske mails fra personer, du ikke kender. Især hvis du ikke plejer at modtage mails på fx engelsk!

Sådan kan du genkende en falsk mail

En falsk mail begynder ofte med en upersonlig indledning for eksempel 'Kære kunde' i stedet for dit navn – afsenderen kender jo ikke dit navn i modsætning til dine venner og andre kontakter.

Typisk indeholder mailen information om, at dit kort har været brugt på en måde, du ikke kan stå inde for eller acceptere. I mailen bliver du derfor opfordret til at klikke på et link, der fører dig til en vellignende kopi af en hjemmeside, hvor du bliver bedt om at indtaste dine oplysninger.

Ofte er mailen forfattet på dårligt dansk, hvilket burde få alarmklokkerne til at ringe. Der er også flere tekniske kendetegn, der kan afsløre, om en mail er falsk. Det hurtigste er at tjekke afsenders domænenavn. I en falsk mail er der oftest små afvigelser, som fx danskkebank.dk, hvor navnet er forkert stavet, eller endelsen er en anden end forventet, fx .cn i stedet for .dk eller lignende. Men der er også tilfælde, hvor domænenavnet ikke umiddelbart afslører, om det er en falsk mail. Heldigvis findes der tekniske muligheder i dit mailprogram, der kan afsløre disse mails.

Men det bedste råd er at have et opdateret antivirus-program, et velfungerende spam-filter og høj sikkerhedsindstilling. Og slipper mailen alligevel forbi din flydespærring, så slet den!

Glem alt om at afgive personlige oplysninger. Og tro ikke på at en tilfældig mail indeholder adgang til en megastor pengepræmie i et lotteri, du ikke har deltaget i!

Herunder kan du se et eksempel på en mail, der tilsyneladende kommer fra Visa. Den fortæller, at du har indtastet din adgangskode til 'Verified by Visa' forkert tre gange, og at du derfor skal indtaste en ny. Det er ikke en rigtig mail fra Visa, men en mail, der forsøger at skaffe kriminelle adgang til fortrolige kortoplysninger. Derfor er der kun én ting at gøre med disse mails - slet dem. Undgå at indtaste dine oplysninger. Visa vil aldrig efterspørge oplysninger på denne måde via en e-mail.

VERIFIED by VISA

MasterCard SecureCode

forkert adgangskode

Du har givet en forkert adgangskode til Verified by Visa er tre gange og skal derfor starte et andet. For at gøre dette, skal du kontrollere dine oplysninger nedenfor. Så snart din nye adgangskode er aktiveret, kan du identificere dig og betale med kortet i Verified by Visa-tilknyttede butikker.

Verified by Visa / MasterCard SecureCode password skal ændres på grund af mange mislykkede logins

Skift dit password!

Har du modtaget en lignende e-mail, skal du

- undlade at besvare e-mailen
- undlade at klikke på linket
- slette e-mailen fra indbakken og papirkurven

Det anbefales, at du opdaterer dit antivirusprogram og efterfølgende foretager en scanning af din pc.

Hvis du allerede har oplyst kortnummer, kontrolcifre og kode, skal du hurtigst muligt sørge for at få spærret det/de kort, du har afgivet oplysninger om.

Og hold øje med din konto og kort – der kan allerede have fundet misbrug sted! De kriminelle er nemlig meget hurtige på tasterne…

Du kan læse meget mere om begrebet på Nets' hjemmeside.

Gildehilsen

Alex R.