



Hva du må gjøre hvis du utsettes for e-postsvindel

Alle kan bli lurt av e-postsvindel. Dette kan være skremmende og ofte føre til panikk. E-postsvindel er også kjent som nettfisking og involverer bruk av e-post og falske nettsteder for å stjele sensitiv informasjon som for eksempel passord, kredittkortnumre, kontodetaljer, adresser og mer.

Bedragerske e-postmeldinger er laget slik at de ser legitime ut, for eksempel meldinger fra banken din eller en annen klarert kilde. De ber deg om å oppgi personopplysninger som deretter kan brukes til identitetstyveri.

Hva skal du gjøre hvis du blir utsatt for e-postsvindel?

ENDRE PASSORD

Hvis du har klikket på feil kobling eller oppgitt personopplysninger som følge av nettfisking, må du endre passordene dine umiddelbart. Dette gjelder e-postkontoer og alle andre kontoer, inkludert bankkontoer og PIN-koder. Opprett nye passord som er sterke og kompliserte og inneholder en rekke tall og symboler. Det er mye vanskeligere for nettkriminelle å knekke slike passord.

VARSLER KREDITTBYRÅER

Ta kontakt med et av de tre største kredittbyråene så snart som mulig og informer dem om at kontoen din kan være kompromittert. Legg inn et svindelvarsel på kontoen til problemet er løst.

KONTAKT KREDITTKORTSELSKAPER

Varsle kredittkortselskapene dine og forklar situasjonen. Kredittkortene er kanskje ikke brukt ennå, men hvis du bekymrer deg for uautoriserte uttak i fremtiden, er det viktig å fryse eller annullere kortene dine. Informer banken om hva som har skjedd, slik at de kan beskytte deg ytterligere.

OPPDATER PROGRAMVAREN DIN

Oppdater programvaren din til den nyeste versjonen og kjør et omfattende virussøk hvis du tror systemet ditt er infisert av virus eller andre skadeprogrammer. Du bør også bruke kryptering, sørge for at du har aktivert en brannmur, og regelmessig sikkerhetskopierte personopplysninger til en ekstern harddisk. Unngå å bruke offentlige Wi-Fi-nettverk når det er mulig, og hvis du må bruke en offentlig tilkobling, bør du velge det sikreste alternativet, for eksempel et virtuelt privat nettverk (VPN). Du bør også slå av datamaskinen når den ikke er i bruk. Den er nemlig utilgjengelig for hackere når den slås av.

SJEKK KONTOENE DINE JEVNLI

Se gjennom bank- og kredittkortkontoene dine regelmessig for å se etter mistenkelige aktiviteter. Du kan også velge å la svindelvarselet stå på kredittvurderingen din litt lenger, til du er helt sikker på at trusselen er eliminert.

RAPPORTERINGSRESSURSER

En rekke ressurser er tilgjengelige for å rapportere e-postsvindel, inkludert National Fraud Information Center. Dette selskapet rapporterer bedragerisk aktivitet til regjeringen og fører en detaljert logg over svindelhendelser. De tilbyr også informasjon om til hvem du kan kontakte for å få hjelp i delstaten din.

ANDRE NYTTIGE RESSURSER OMFATTER:

Internet Crime Complaint Center: FBI og National White Collar Crime Center driver et nettsted som heter Internet Crime Complaint Center. Det tilbyr mange tips og annen nyttig informasjon om hvordan du unngår e-postsvindel og hva du skal gjøre hvis du utsettes for slik svindel. Det har også en kobling du kan bruke for å legge inn en klage mot en tredjepart som har stjålet identiteten din eller har gjort forsøk på det. **Det amerikanske justisdepartementet:** Det amerikanske justisdepartementet kjører nettsteder som lar deg legge inn klager om e-postsvindel. Nettstedet har også mange nyttige tips og råd. **National Consumer League:** Dette nettstedet kan hjelpe deg med å legge inn en klage og gir deg informasjon om hvordan du kan unngå svindel. **Better Business Bureau (BBB):** BBB lar deg varsle andre om hva som skjedde med deg, slik at de ikke faller for de samme svinforsøkene. Vær proaktiv til du er helt sikker på at antallet svindelrelaterte problemer er betydelig redusert, og du vet hva du skal se etter i fremtiden. Jo mer du lærer om nettfisking og annen Internett-svindel, jo mindre sannsynlig er det at slike problemer vil oppstå. 

