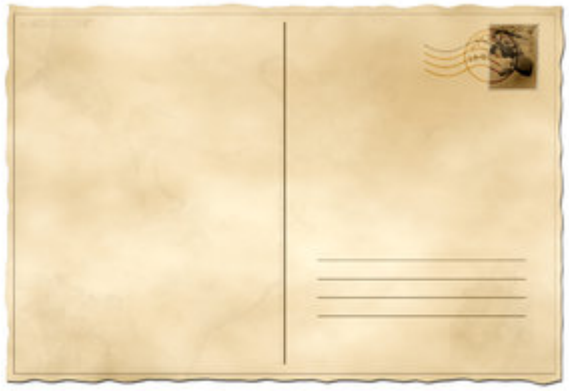
INFORMASIETEGNOLOGIE

INFORMATION TECHNOLOGY

TEKEN IN, TEKEN UIT



Een van die algemeenste vrae wat gebruikers vir ons vra is - Hoe kry gemorsposversenders my e-posadres? Vorige kere het ons gekyk na Repelsteeltjie-aanvalle, robotte, trojane en zombies. Hierdie keer fokus ons op `n derde metode - die inteken/uitteken opsie van nuusbriewe.

In die 21ste eeu kan daar gesê word "Kennis is mag, nie geld nie ". Hierdie twee is egter baie naby aan mekaar. Kennis of "data" is `n gewilde gebruiksartikel op die internet. Facebook het byvoorbeeld meer as 1.2 biljoen gebruikers. Dink net aan die waarde van al daardie data as Mark Zuckerberg (stigter van Facebook) besluit om die inligting te verkoop?

Jy sal dikwels `n e-pos ontvang in die vorm van `n nuusbrief met `n skakel onderaan wat gemerk is met "Unsubscribe" en aan jou die geleentheid gee om uit te teken, maar gaan die e-posse ophou as jy daarop kliek?

Ongelukkig is daar vele gewetenlose nuusbrief-versenders wat jou adres vir `n lekker vet kommissie sal verkoop. `n Algemene "unsubscribe" taktiek is om `n e-pos na miljoene mense te stuur met `n bedrieglike “you have joined a newsletter” e-pos. Wanneer gebruikers kliek op die “unsubscribe”-skakel, teken hulle nie uit nie, maar bevestig onwetend dat hulle `n regte persoon is met `n aktiewe e-posadres.

Hierdie aksie veroorsaak nog meer gemorspos en binnekort oorstroom jou posbus. Daarbenewens sal gemorspos-versenders ook hul databasis (wat jou "bevestigde "adres insluit) aan ander gemorspos-verspreiders en bemarkingsfirmas stuur.

`n Ander metode om e-posadresse in die hande te kry is deur wettige nuusbriewe. Jy skryf dalk dikwels in vir `n regmatige nuusbriefdiens en ontvang die nuusbriewe op `n gereelde basis. Wanneer jy egter jou persoonlike inligting en kontakdetails in `n derde party (die nuusbrief-diens) se hande vertrou, maak jy staat daarop dat hulle stelsel en databasis sekuriteit voldoende is en nie kwesbaar is vir kodebreking of identiteitsdiefstal nie. Kodebrekers kan die nuusbriefdiens se e-pos databasis steel en sonder moeite is jou adres in die hande van gemorsposversenders en swendelaars.

In sommige gevalle samel bemarkers en nuusbriefdienste e-posadresse en verkoop dit aan `n derde party. Ongelukkig het jy waarskynlik vir hulle toestemming gegee toe jy ingestem het tot hulle voorwaardes, soos gestipuleer in die “Terms & Conditions” toe jy ingeskryf het vir die diens. Daar word dikwels aangedui dat jy aan die diens die reg gee om jou inligting met hulle vennote te deel, wat jou om die beurt weer mag kontak.

Onthou hierdie paar belangrike wenke:

- *Opnames genereer baie gemorspos. Menige mense neem deel aan opnames vir `n ekstra inkomste, gratis geskenke, ens, maar jou details word dikwels deurgegee aan bemarkers vir verdere gebruik.*
- *Poog om jou gemorspos tot `n minimum te beperk deur nie jou adres vir enigiemand te gee wat jy nie ken of vertrou nie. Moet ook nie dieselfde adres wat jy vir besigheiddoeleindes, soos jou internetbankdienste gebruik vir nuusbriewe nie.*
- *Verskillende gemorspos kom dikwels vanaf dieselfde bron. Sodra jy begin uitteken, sal jy sien dat die uitteken-webblad telkens dieselfde lyk.*

- *Indien jy inligting op `n webwerf probeer kry en die blad vra vir `n e-posadres, probeer abc@123.com of iets soortgelyk aan jou adres eerder as jou regte adres. Ten minste word JOU adres nie op rekord gehou en later misbruik nie.*
- *As jy jou inskrywing gekanselleer het en jy kry steeds gemorspos, blokkeer die stuurder se adres of domein by Outlook se "junk mail"-opsie.*

[INLIGTING VERSKAF DEUR DAVID WILES]

Posted in:E-pos,Sekuriteit | Tagged:Nuusbriewe | With 0 comments