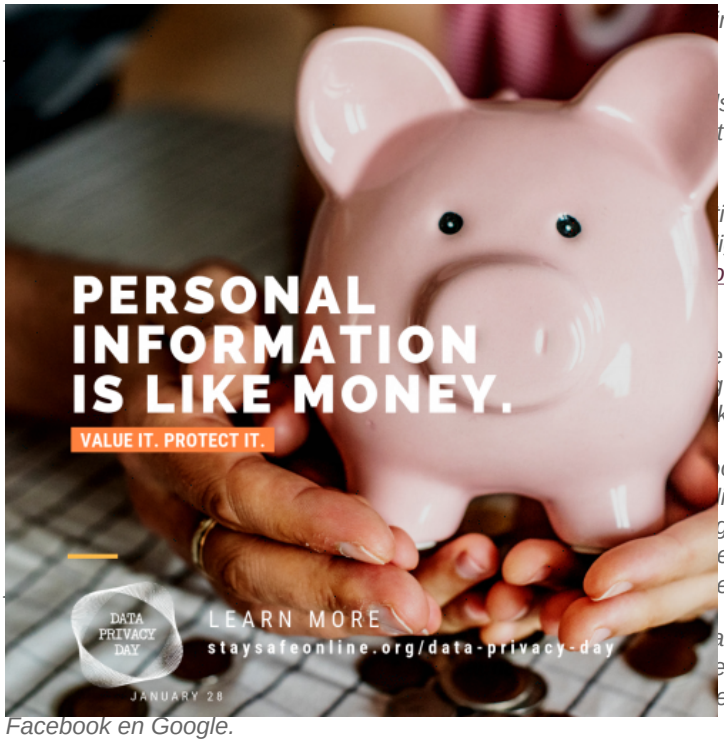
INFORMASIETEGNOLOGIE

INFORMATION TECHNOLOGY

ELKE DAG IS DATABESKERMINGSDAG



nisiatief is reeds sedert 2007 aktief in Europa en twee

'sdag (in Europa ook bekend as Databeskermingsdag) t word tans erken in Amerika, Kanada, Israel en 47

ien jaar, het bewustheid oor die beskerming van data ig. Eerstens was daar die afgelope tyd ? stuwing in ogle wat met £44 miljoen in Frankryk beboet is vir

e jaar. Voorheen was maatskappye nie wetlik verplig het dit verander. Maatskappye word tans kliënte se inligting blootstel.

of Uitvoerende Beampte by OpenText, bou ons elke it eers weet. Hierdie digitale voetspoor maak dit gebruikersname en wagwoorde is, jou fisiese es spoor jou aksies na en voorsien jou optrede voordat entjie en kan tot jou nadeel gebruik word.

ak dat jy self verantwoordelikheid neem vir die e of sosiale netwerke om ons digitale identiteit veilig te elope jaar – insluitende groot maatskappye soos Facebook en Google.

Databeskermingsdag is net een dag in die jaar waar dataeienaars (dis elkeen van ons wat digitale platforms gebruik) bewus gemaak kan word van die belangrikheid van data. Ons moet egter elke dag bewus wees van die risiko's. Hoe kan jy jou data beskerm? Jy weet reeds, jy moet dit net begin doen of beter doen. www.digitalguardian het ? deeglike gids oor databeskerming, maar hier is 10 wenke om mee te begin:

1. *Gebruik netwerke met enkripsie wanneer jy toegang nodig het tot belangrike inligting. Oop en gratis Wi-Fi is handig, maar dit kom met risiko's. Indien jy webwerwe besoek wat nie https gebruik nie, onthou dat jou data deur enigiemand anders gesien en misbruik kan word.*
2. *Kies sterk wagwoorde. Weet nie hoe nie? Hier is ? paar wenke. Daar is ? neiging na twee-faktor bekragtiging en meer sekuriteitsdeskundiges beveel sagteware aan wat jou wagwoorde bestuur.*
3. *Beskerm jou wagwoorde. Moet dit nie neerskryf nie. Moet dit nie deel nie. Moet ook nie dieselfde wagwoord gebruik vir al jou sosiale netwerke of ander webwerwe nie.*
4. *Dateer jou sagteware op wanneer dit jou aanhits. Moet dit nie ignoreer omdat jy haastig is nie – dit kan ? belangrike sekuriteitsopdatering insluit.*
5. *Dateer gereeld jou anti-virus sagteware op. Nuwe weergawes van virusse, malware, ens. word op ? daaglikse basis vrygestel. As jy dit nie opdateer nie, word jy ? maklike teiken. Oorweeg ook anti-virus sagteware vir jou mobiele toestelle – hulle is selfs meer kwesbaar as jou rekenaars.*
6. *Gaan die privaatheidverstellings op jou slimfoon na. Oorweeg versigtig vir watter toepassings jy toegang wil gee tot sekere funksies op jou foon.*
7. *Sluit jou slimfoon en tablet wanneer jy dit nie gebruik nie. Mobiele toestelle word meer gereeld gebruik vir toegang*

tot sosiale media, bankdienste en minder veilige toepassings wat maklik misbruik kan word as iemand toegang kry.

8. *Aktiveer die “remote location” en die toestel-skoonvee funksies. Indien jou mobiele toestel gesteel word, kan iemand ten minste nie toegang tot jou inligting ook kry nie.*
9. *Verwyder al jou data van ou toestelle, byvoorbeeld ou slimfone wat verkoop, weggegooi of vir iemand anders gegee word.*
10. *Laastens, maak seker jy rugsteun jou data op ? gereelde basis. Ten minste sal jy steeds toegang hê, al verloor jy jou toestel.*

Data is mag en as jy die mag in jou hande wil hou, moet jy dit beskerm.

[BRONNE: https://www.forbes.com; https://www.techradar.com]

Posted in:Academic IT,Sekuriteit | Tagged:Data Privacy,Data Privacy Day,GDPR | With 0 comments