Praktikat më të mira për privatësinë e të dhënave për përdoruesit fundorë

Çfarë është privatësia e të dhënave?

Privatësia e të dhënave i referohet masës në të cilën të dhënat sensitive të një përdoruesi fundor ndahen me palët e treta në internet. Të dhënat sensitive mund të përfshijnë (por nuk kufizohen në) emrin e një individi, adresën, datën e lindjes, racën, gjininë, informacionin e kontaktit, numrin e kartës së kreditit, fotografinë, numrin e identitetit, adresën IP ose të dhënat e vendndodhjes.

Të dhëna sensitive janë çdo e dhënë që lidhet me sjelljen në botën reale ose në internet të një individi, qoftë ky një transaksion financiar në një faqe të tregtisë elektronike (e-commerce) ose një veprim (p.sh., një pëlqim ose shpërndarje) të një postimi në mediat sociale.

Një përdorues fundor është një individ që përdor harduer ose softuer të programuar ose krijuar nga një person tjetër që nuk e mirëmban atë produkt.

Në vendet e BE-së po dhe në vendet që kanë filluar negociatat sic është Shqipëria, privatësia e të dhënave konsiderohet si një e drejtë themelore, e mbrojtur nga rregullore strikte sic eshte rregullorja mjaft e njohur, Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave të Bashkimit Evropian (GDPR), e cila detajon të drejtat e subjekteve të të dhënave.

Privatësia e të dhënave është po aq e rëndësishme për ndërtimin e besimit me klientet globalë bazuar në përpunimin, ruajtjen dhe ndarjen e informacionit të tyre. Nëse këto të dhëna nuk sigurohen, një organizatë jo vetëm që i vë të dhënat e klientëve të saj në rrezik të rrjedhjes së të dhënave, por gjithashtu duhet të paguajë edhe detyrimet dhe gjobat rregullatore.

Praktikat më të mira për privatësisë së të dhënave për përdoruesit fundorë

Për të mbajtur informacionet sensitive të sigurta në çdo kohë, përdoruesit fundorë duhet të ndjekin praktikat më të mira të mëposhtëme të privatësisë së të dhënave që sigurojnë informacionin si në jetën e tyre personale ashtu edhe në atë profesionale.

1. Duhet të dijë se çfarë konsiderohet informacion personal

Informacioni personal është çdo informacion që mund të përdoret në mënyrë të pavarur ose me informacione të tjera për të identifikuar një individ. Ajo përfshin:

- Emri, adresa dhe data e lindjes,
- Numri i pasaportës ose patentës së shoferit
- Histori mjekësore, kriminale ose financiare
- Origjina etnike ose racore
- Adresa IP, nëse mund të gjurmohet një individ
- ADN-ja, gjurmët e gishtërinjve dhe të zërit

Për të mbrojtur këtë informacion dhe çdo lloj tjetër informacioni personal, përdoruesi fundor duhet ti ndajë me të tjerët kur është absolutisht e nevojshme dhe vetëm me marrësit që njeh dhe i beson.

2. Të ketë kujdes nga sulmet phishing

Emailet phishing janë një nga kërcënimet më të rëndësishme për informacionin personal. Kriminelët kibernetikë e përdorin këtë sulm për të mashtruar individët që të klikojnë në një link të dyshuar ose të shkarkojnë një skedar keqdashës për të vjedhur të dhënat e tyre ose për të instaluar malware në pajisjen e tyre.

Për t'u mbrojtur kundër këtyre emaileve, duhet:

- Të shmanget hapja e emaileve nga dërgues të panjohur. Nëse dyshohet se dërguesi është i panjohur, mund të hetohet më tej përmes telefonit.
- Nuk duhet klikuar në linket e emaileve të dërguar nga persona të panjohur, pasi mund të drejtojnë në një faqe interneti phishing ose të shkarkojnë programe keqdashëse në pajisjen e tyre.
- Nuk duhet tu kthehet përgjigje emaileve që kërkojnë të dhëna konfidenciale ose personale. Asnjë organizatë me reputacion nuk do të kërkojë informacion personal me email.
- Nëse diçka tingëllon shumë e mirë për të qenë e vërtetë, ndoshta është e tille, prandaj duhet injoruar çdo email që njofton se është fituar një çmim ose është përfituar një ulje speciale.

3. Të ketë kujdes nga sulmet për vishing dhe smishing

Kriminelët kibernetikë nuk përdorin vetëm email-et për të mashtruar viktimat për të marrë informacionine personale. Ata gjithashtu përdorin mesazhe SMS (smishing) dhe mesazhe zanore (vishing).

4. Të merren hapa për të siguruar blerjet online në faqet e tregtisë elektronike

Blerja në internet është një pjesë e jetës së përditshme të shumë njerëzve, prandaj është një objektiv kryesor për kriminelët kibernetikë. Ndaj është jetike të ndërmerren hapa shtesë për të mbrojtur të dhënat kur përdoret një faqe e tregtisë elektronike ose një platformë transaksionesh të palëve të treta.

Blerja në internet bëhet më e sigurtë duke ndërmarrë veprimet e mëposhtme:
• Të sigurohet që faqja e tregtisë elektronike është legjitime.
Gjëja e parë që duhet të bërë kur bëhet një blerje në një faqe të re të tregtisë elektronike është të kontrollohet legjitimiteti i tij duke bërë si më poshtë:

- Të kontrollohet URL-ja, duke u siguruar që ajo fillon me "HTTPS", gjë që tregon se ka një komunikim të koduar midis shfletuesit dhe gjithashtu të kontrollohet se në fushen e URL-se ka një dryn të mbyllur gjë që tregon që transaksioni është i sigurtë.
- Të kontrollohet certifikata e sigurisë së faqes së tregtisë elektronike – Në disa shfletues, klikohet në ikonën e drynit dhe del një opsion që shkruan “Shfaq certifikatën” për të parë se nga kush është lëshuar certifikata dhe kur skadon.

• Të ketë kujdes nga vjedhjet e identitetit dhe mashtrimet e lidhura me to. Përdoruesit duhet të jenë të përgatitur për të dalluar mashtrimet për të marr informacione personale.

• Të përdoret autentifikimi me shumë faktorë kudo që ofrohet. Shumë dyqane online kërkojnë të krijohet një llogari përpara blerjes. Për këtë duhet krijuar një fjalëkalim i fortë dhe të konfigurohet autentifikimi me shumë faktorë nëse ofrohet.

5. Të mos përdoret Wi-Fi publik

Përdorimi i Wi-Fi publik për të blerë në internet mund të jetë i përshtatshëm për të bërë blerje impulsive dhe urgjente. Megjithatë, mund të rrezikojë informacionin personal, pasi hakerat mund të përgjojnë të dhënat e transmetuara në të gjithë rrjetin. Kjo do të thotë që nuk duhet të transmetoni kurrë adresën tuaj dhe informacionin e kartës së kreditit në një lidhje publike Wi-Fi.

Nëse duhet patjetër të blini në internet ndërsa jeni të lidhur me një pikë aksesi publike Wi-Fi, duhet përdorur një Rrjet Virtual Privat (VPN) për të mbrojtur të dhënat tuaja, në mënyrë që ato të mos gjurmohen dhe të merren nga kriminelët kibernetikë.

6. Të raportohen kërkesat e dyshimta për informacion personal

Filtrat e postës elektronike dhe masat e tjera paraprake teknike nuk sigurojnë automatikisht privatësinë e të dhënave personale. Nëse vihet re ndonjë mesazh ose aktivitet i dyshimtë që mund të ketë kompromet uar informacionin personal, duhet raportuar menjëherë tek departamenti i IT-së ose tek autoritetet përkatëse.

7. Pjesëmarrje në trajnime ndërgjegjësuese për sigurinë e informacionit

Organizatat dhe individët që trajtojnë të dhënat personale të të tjerëve duhet të përdorin praktikat më të mira të privatësisë së të dhënave. Për të mbrojtur plotësisht të gjitha informacionet, të gjithë duhet të kryejnë të paktën një lloj trajnimi ndërgjegjësuese rreth sigurisë se informacionit. Duhet të përvetësohen njohuritë që nevojiten për të mbajtur të dhënat të sigurta dhe gjithashtu për të krijuar dhe forcuar zakone të mira në internet.