

Udhëzues për përdoruesit rreth incidenteve të sigurisë

Për të mbrojtur klientët e saj dhe në zbatim të Rregullores Nr.37 datë 29.10.2015 “MBI MASAT TEKNIKE DHE ORGANIZATIVE PER TE GARANTUAR SIGURINE DHE INTEGRITETIN E RRJETEVE DHE/OSE SHERBIMEVE TE KOMUNIKIMEVE ELEKTRONIKE”, shoqëria Soft & Solution, publikon këtë udhëzues për përdoruesit “**Rreth incidenteve më të zakonshme të sigurisë, veprimeve dhe/ose mjeteve që duhen ndjekur për të parandaluar ndodhjen e këtyre incidenteve dhe veprimeve që duhen ndjekur pas ndodhjes së incidenteve të sigurisë**”

Me qëllim mbrojtjen tuaj nga aktivitete me natyrë mashtruese në fushën e komunikimeve elektronike, Soft & Solution sugjeron :

1. Krijoni fjalëkalim të fortë

Që një fjalëkalim të jetë sa më i sigurtë duhet që të siguroheni që përmban minimalisht tetë karaktere, ndër të cilat numra, gërma të mëdha dhe të vogla si dhe simbole. Nuk është e këshillueshme që të përdorni të njëjtin fjalëkalim kudo dhe ta ndani me të tjerët.

2. Kujdes nga e-mail-et mashtruese

Jeni të lutur të mos ju përgjigjeni email-eve mashtruese të cilët vijnë nga kontakte të panjohura dhe kërkojnë informacion për të dhënat tuaja personale, si kartë krediti, numra llogarie etj. Gjithashtu duhet të tregoni kujdes në hapjen e link-eve të ndryshëm në internet.

3. Mbroni pajisjet tuaja

Aktivizoni firewall dhe antivirus në kompjuter për mbrojtjen e navigimit tuaj në internet. Gjithmonë vendosni fjalëkalim për lidhjen me wireless.

4. Kujdes nga telefonatat mashtruese

Ju lutemi, mos telefononi numra ndërkombëtarë të cilët nuk i njihni sepse këta numra mund të rezultojnë me tarifa tepër të larta. Mashtruesit që gjenerojnë këto thirrje të humbura synojnë që ju të merrni mbrapsht këto numra shumë të kushtueshëm ndërkombëtarë.

5. Përdorimi i kujdesshëm i rrjeteve sociale

Menaxhoni privatësinë në rrjetet sociale duke zgjedhur se cilët mund të shohin profilin tuaj. Kontrolloni postimet që ju bëni. Mos publikoni foto të fëmijëve tuaj të cilat japin informacion mbi vendndodhjen e tyre. Përzgjidhni me kujdes personat që zgjidhni të bëni miq dhe bllokoni hyrjet e padëshiruara.

6. Kujdes kur lidheni me wireless-a që janë pa password

Mos vendosni të dhënat tuaja personale dhe passwordet tuaja kur lidheni me wireless që janë pa password pasi faqet mund të duken sikur janë njësoj por mund të marrin të dhënat tuaja personale. Ju këshillojmë që të përdorni programe VPN .