Néhány jó tanács, hogy ne váljon online csalók áldozatává:

1. Gondolja át a kapott üzenet tartalmát. Tisztázza magában, hogy a leírtak mennyire feleltethetőek meg a valóságnak. Lehet, hogy az adott szolgáltatásnak vagy banknak nem is az ügyfele? Egy olyan szolgáltatástól kap sms-t, ahol korábban nem adta meg a telefonszámát? Nem is rendelt semmit, mégis hogyan érkezhetne csomagja?
2. Amennyiben nem tudja eldönteni egy üzenet valóságtartalmát, vegye fel a kapcsolatot a küldővel. Keresse fel például a szolgáltatója, a bankja vagy a hivatkozott csomagküldő szolgálat hivatalos honlapját, esetleg hívja fel őket a hivatalos telefonszámukon. Amennyiben egy közösségi oldalon privát üzenetet kap egy ismeretlentől? Hagyja figyelmen kívül. Azonban ha egy ismerőstől, kérdezzen vissza a linkre kattintás előtt, mit küldött Önnek az illető.
3. Mindig legyen gyanakvó a mások által kezdeményezett olyan kapcsolatfelvétellel szemben, amikor nem tud minden kétséget kizáróan megbizonyosodni a másik fél kilétéről. Ne adja meg illetékteleneknek személyes, pénzügyi és biztonsági adatait! Ha egy gyanús üzenet egy linket vagy egy mellékletet tartalmaz, ne kattintson rá és ne is töltse le.
4. Az esetek túlnyomó többségében az online térben működő bűnözők az emberi kíváncsiságot használják ki. Ne dőljön be egy ismeretlen feladótól kapott üzenetnek, ne akarjon csak most az egyszer kattintani, még akkor sem, ha az üzenet szerint egy videót talált Önről egy ismerőse. Egy nem várt és minden előzmény nélkül kapott linket vagy csatolmányt ne nyisson meg.
5. Amennyiben adathalász-támadás célpontjává vált, jelezze ismerőseinek, ezzel segítve az ő online biztonságukat. Nem volt elég szemfüles egy adathalász-üzenet kapcsán, és rákattintott az abban található linkre? Haladéktalanul vegye fel a kapcsolatot a számlavezető bankjával, és tegyen feljelentést a rendőrségen!
6. Ne kattintson kéretlen szöveges üzenetekben érkezett hivatkozásokra, mellékletekre vagy képekre a küldő személyazonosságának ellenőrzése nélkül! Az ellenőrzéshez keressen rá a számra az interneten (ha csalásról van szó, valószínűleg nem Ön lesz az első), vagy hasonlítsa össze a számot az érintett szervezet hivatalos telefonszámával!
7. Azonnal vegye fel a kapcsolatot a bankjával, ha azt gyanítja, hogy egy smishing üzenetre válaszolt és megadta banki adatait!