KEDVEZŐ AJÁNLAT vagy ÁTVERÉS?

Az online vásárlás aranyszabályai

MEGBÍZHATÓ FORRÁSBÓL VÁSÁROLJON!

Válasszon olyan márkákat és üzleteket, amelyeket ismer!

ELLENŐRIZZE A VÉLEMÉNYEKET ÉS ÉRTÉKELÉSEKET!

Különösen ismeretlen üzletek és egyéni eladók esetében.

ELLENŐRIZZE AZ ISMÉTLŐDŐ DÍJAKAT!

Mielőtt megadná a bankkártyája adatait az interneten keresztül egy folyamatos szolgáltatás kifizetéséhez, tudja meg, hogyan mondhatja le a szolgáltatást!

GYŐZŐDJÖN MEG AZ ADATÁTVITEL BIZTONSÁGÁRÓL!

Használjon HTTPS és SSL protokollokat böngészéskor. Emlékezzen: a lakat szimbólum önmagában nem tesz egy honlapot törvényessé.

GONDOLJA ÁT KÉTSZER, MIELŐTT FIZET!

Legyen tisztában az online vásárlás kockázataival!

HASZNÁLJON HITELKÁRTYÁT, AMIKOR ONLINE VÁSÁROL!

A legtöbb bankkártyát erős ügyfélvédelmi szabályzat óvja. Ha nem kapja meg, amit megrendelt, a kártyakibocsátó bank megtéríti Önnek az árát.

MENTSE EL AZ ÖSSZES, ONLINE VÁSÁRLÁSHOZ KAPCSOLÓDÓ DOKUMENTUMOT!

Ezekre szükség lehet az adásvétel körülményeinek megállapításához vagy annak igazolásához, hogy kifizette az árut.

NE KÜLDJÖN PÉNZT ISMERETLEN SZEMÉLYNEK!

Ha az utcán nem adna pénzt egy ismeretlen személynek, ne tegye ezt az interneten sem! Ha lehetséges, először kapja meg az árut, utána fizessen!

SOHA NE KÜLDJE EL A BANKKÁRTYÁJA ADATAIT E-MAILEN!

Soha ne küldjön másolatot a kártyájáról, a PIN kódjáról, vagy más kártyainformációról e-mailen!

NEM VÁSÁROL? NE ADJA MEG A KÁRTYADATAIT!

Ha nem vesz semmit, ne továbbítsa és ne mentse el a bankkártyaadatait!

ELLENŐRIZZE A WEBOLDAL FIZETÉSI BIZITONSÁGÁT!

Csak olyan weboldalon vásároljon, amely teljes azonosítási rendszert használ (mint a Verified by Visa / MasterCard Secure Code)

EUROPOL EC3 European Cybercrime Centre

MRC

Rendőrség Police

Nemzeti Nyomozó Iroda NNI

Magyar Bankszövetség

#BuySafePaySafe

CSAK MEGBÍZHATÓ ALKALMAZÁSOKAT TELEPÍTSEN!

Csak hivatalos alkalmazásboltból telepítsen mobil-eszközére alkalmazást!

Üzenetben kapott linkről soha ne töltsön és telepítsen alkalmazást, még akkor sem, ha ismerőse kéri!

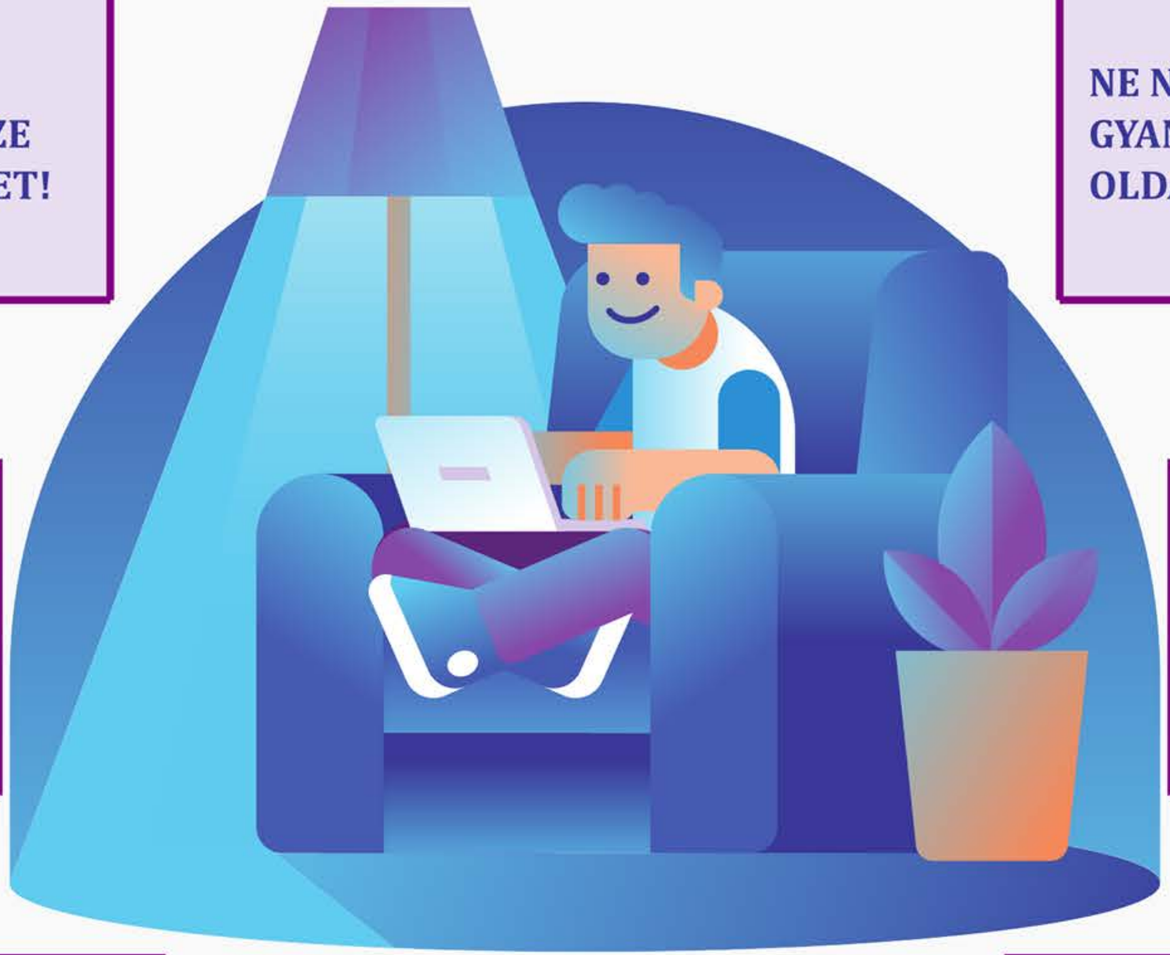
Egyes alkalmazok távoli hozzférést biztosítanak eszközeihez és az azon tárolt összes fájlhoz, jelszóhoz! Legyen nagyon óvatos!

Ha nem tudja pontosan egy alkalmazásról, hogy mire használható, ne telepítse mobileszközére!

ALAPOSAN ELLENŐRIZZE AZ URL CÍMET!

NE NYISSON MEG GYANÚS OLDALAKAT!

HASZNÁLJON ERŐS JELSZAVAKAT!



CSAK MEGBÍZHATÓ ALKALMAZÁSOKAT TELEPÍTSEN!

VÁLASSZON BIZTONSÁGOS FIZETÉSI MEGOLDÁSOKAT!

VÉDEKEZZEN A KIBERTÁMADÁSOK ELLEN!

CSAK BIZTONSÁGOS HÁLÓZATOKAT HASZNÁLJON!

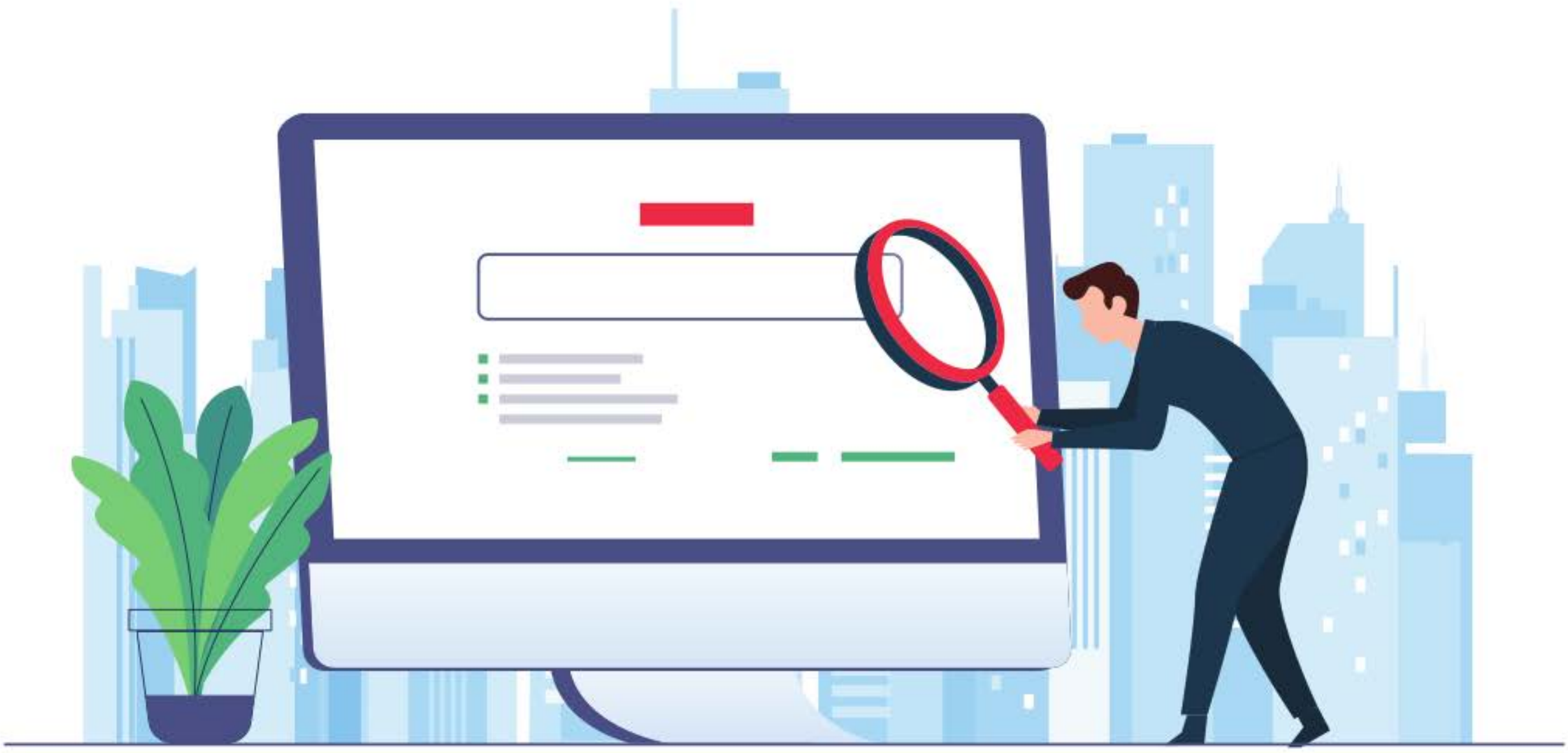
VIGYÁZAT, CSALÓK!

Telefonon SOHA ne adja meg:
- bankkártyája vagy
- netbankja belépési adatait!

Ne telepítsen ismeretlen programot számítógépére, telefonjára!

Akkor sem, ha a bankja nevében, a bankja telefonszámáról telefonáló személy kéri!

Ha a hívó valamilyen bankkártyával vagy bankszámlával kapcsolatos problémára hivatkozik, szakítsa meg a hívást, és hívja fel Ön a bank ügyfélszolgálatát!



ELLENŐRIZZE A WEBOLDAL CÍMÉT!

Üzenetben kapott linkre kattintás előtt ellenőrizze, hogy a link valóban arra az oldalra mutat, ahogy látszik!

Vigye a kurzort a link fölé:
- a levelezőprogramban egy felugró ablakban,
- a böngészőben pedig az oldal alján megjelenik a tényleges cím.

Ha link máshova mutat, mint ahogy az a szövegben látszik, ne nyissa meg a hivatkozást!

Megnyitást követően ellenőrizze a böngésző címsorában, hogy valóban a megfelelő oldalra jutott!

FIGYELEM!

Ne dőljön be az ismeretlen feladótól vagy látszólag a saját címéről érkező e-mailnek, amely azzal fenyegeti, hogy kamerafelvételeket, levelezését vagy egyéb üzeneteit közzéteszi!

NE KÜLDJÖN PÉNZT (BITCOINT) A MEGADOTT TÁRCÁRA!

ZSAROLÓ E-MAIL ÁTVERÉS