

# RENĐŐRSÉGI FELHÍVÁS

## ONLINE CSALÁSOK MEGELŐZÉSÉRE



[www.kiberpajzs.hu](http://www.kiberpajzs.hu)

# FELHASZNÁLÓI FIÓKOK VÉDELME



## Felhasználói fiókjai

(levelezés, közösségi oldalak, online tárhelyek és egyéb szolgáltatások) védelme érdekében:

- Használjon minden oldalon eltérő, **ERŐS JELSZAVAKAT!**
- Jelszavai biztonságos tárolásához használjon **JELSZÓKEZELŐ ALKALMAZÁST!**
- Ahol lehet, állítson be **KÉTFAKTOROS HITELESÍTÉST!**

## Az ajánlott jelszó:

- hosszú, min. 12 karakter
- összetett: kisbetűk, nagybetűk, számok, speciális karakterek
- nem kötődik semmilyen formában a felhasználóhoz
- Például: \$#Q!4o2Tv6x\$

# ADATHALÁSZAT MEGELŐZÉSE

- Mindig ellenőrizze az e-mail feladóját!
- Alaposan olvassa el az e-mailt. Figyeljen a helyesírási hibákra, ékezetek hiányaira!
- Üzenetben kapott linkre kattintás előtt ellenőrizze, hogy a link valóban arra az oldalra mutat, ahogy látszik!
- Megnyitást követően ellenőrizze a böngésző címsorában, hogy valóban a megfelelő oldalra jutott-e!



# BANKI TELEFONOS CSALÁSOK MEGELŐZÉSE

Bankok nevében, látszólag a bank telefonszámáról telefonáló csalók próbálják megszerezni az ügyfelek személyes és pénzügyi adatait. A csaló jogosulatlan bankkártya-használatra vagy átutalásra hivatkozik.

- A beszélgetés elején kérdezze meg, hogy kit keres, ha a telefonáló nem tudja az Ön pontos nevét, akkor szakítsa meg a hívást!
- Semmilyen programot ne telepítsen és ne utaljon pénzt biztonságosnak mondott bankszámlára még a bank nevében telefonáló személy kérésére sem!
- Személyes vagy banki adatot, ideértve a bankkártya-adatokat is, ne osszon meg senkivel telefonon! Ha valóban a bank ügyintézője telefonál, ő ismeri a szükséges adatokat.



**AZ ÖN PÉNZE BIZTONSÁGBAN VAN, AMÍG MÁSNAK NEM BIZTOSÍT HOZZÁFÉRÉST A BANKSZÁMLÁJÁHOZ. HA KÉTSÉGEI TÁMADNAK A HÍVÁSSAL KAPCSOLATBAN, SZAKÍTSA MEG AZT ÉS HÍVJA FEL ÖN A BANK ÜGYFÉLSZOLGÁLATÁT!**