ՅՈՒՆԻԲԱՆԿ

ՏԵՂԵԿԱՏՎԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ

ԻՐԱՋԵԿՈՒՄ ՀԱՃԱԽՈՐԴՆԵՐԻ ՀԱՄԱՐ

ՅՈՒՆԻԲԱՆԿ

ՖԻՇԻՆԳ

Ի՞նչ է ֆիշինգը

Ֆիշինգը կիբեռհարձակում է, որի ընթացքում խարդախները ներկայանում են որպես վստահելի կազմակերպություն՝ ձեր անձնական տվյալները գողանալու նպատակով:

Ինչպես է աշխատում ֆիշինգը

1. Հարձակվողը ներկայանում է որպես բանկ, ընկերություն կամ ծառայություն

2. Ուղարկվում է կեղծ նամակ, SMS, հաղորդագրություն կամ հղում

3. Ձեզ ստիպում են արագ արձագանքել

4. Դուք տեղափոխվում եք կեղծ, բայց իրականին նման կայք

5. Ձեր տվյալները անմիջապես գողացվում են

6. Տվյալները օգտագործվում կամ վաճառվում են

ՅՈՒՆԻԲԱՆԿ

ՖԻՇԻՆԳԻ ՏԱՐԱԾՎԱԾ ՏԵՍԱԿՆԵՐ

Էլ. փոստի ֆիշինգ

Կեղծ նամակներ

Թիրախային ֆիշինգ

Անհատականացված հարձակումներ

SMS ֆիշինգ (Smishing)

Կեղծ հաղորդագրություններ

Հեռախոսային ֆիշինգ (Vishing)

Կեղծ զանգեր

Կլոն ֆիշինգ

Փոփոխված իրական նամակներ

Ինչպես պաշտպանվել

- ✓ Մի սեղմեք կասկածելի հղումների վրա
- ✓ Միշտ ստուգեք ուղարկողի հասցեն
- ✓ Օգտագործեք երկքայլ հաստատում (2FA)
- ✓ Թարմացրեք ձեր համակարգերն ու ծրագրերը
- ✓ Մի տրամադրեք անձնական տվյալներ անծանոթ աղբյուրներին

Հիշեք. Եթե հաղորդագրությունը ձեզ շտապեցնում է կամ վախեցնում՝ մեծ հավանականությամբ դա խաբեություն է:

ՅՈՒՆԻԲԱՆԿ

ԱՊԱՀՈՎ ԳԱՂՏՆԱԲԱՌԻ ՈՒՂԵՑՈՒՅՑ

Երկարություն

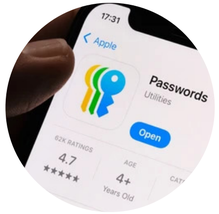
Օգտագործեք առնվազն 12 նիշ և ավելի

Եզակիություն

Մի՛ կրկնօրինակեք այլ անձանց գաղտնաբառեր

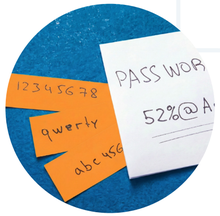
Բարդություն

Ներառեք փոքրատառեր և մեծատառեր, թվեր և հատուկ նիշեր



Պահեստավորում

Օգտագործեք գաղտնաբառերի մենեջեր և խուսափեք դրանք բացահայտ պահելուց



Անորոշություն

Խուսափեք տարածված բառերից, անուններից կամ ամսաթվերից

Հաճախականություն

Խուսափեք նույն գաղտնաբառերը օգտագործելուց

Պատահականություն

Ստեղծեք կամ օգտագործեք գաղտնաբառեր, որոնք լիովին պատահական են

Կիսվել

Երբեք մի՛ կիսվեք գաղտնաբառերով որևիցե մեկի հետ անկախ պատճառից

ՅՈՒՆԻԲԱՆԿ

Էլ. ՓՈՍՏԻ ԱՆՎՏԱՆԳ ՕԳՏԱԳՈՐԾՄԱՆ ՊՐԱԿՏԻԿԱ

1. Երբեք մի՛ բացեք անհայտ կամ կասկածելի աղբյուրներից ստացված հղումներ կամ կից ֆայլեր

2. Ուշադրություն դարձրեք կասկածելի արտահայտություններին, քերականական և ուղղագրական սխալներին

3. Զգուշացեք գայթակղիչ բովանդակություն պարունակող առաջարկներից, որոնք չափազանց գրավիչ են իրական լինելու համար

4. Հաղորդեք ֆիշինգային էլ. փոստերի մասին՝ ֆիլտրերը բարելավելու համար

5. Համոզվեք, որ գործում են անվտանգության հետևյալ միջոցները՝ DMARC, SPF և DKIM

6. Կարգավորեք էլ. փոստերի ավտոմատ սկանավորումը և սպառնալիքների զտումը

ՅՈՒՆԻԲԱՆԿ

Տեղեկատվական
անվտանգության դեպարտամենտ
(+374) 43 004 105