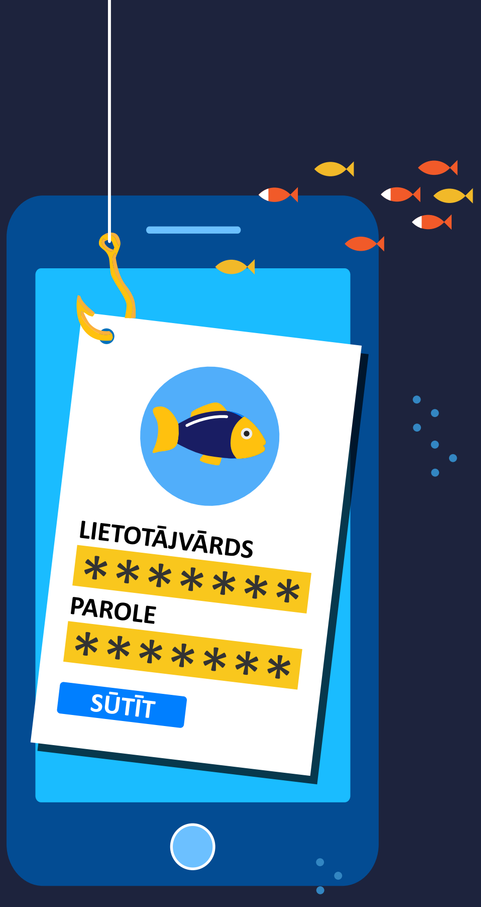
APDRAUDĒJUMS TĪMEKLĪ

PĀRBAUDIET DIVREIZ PIRMS KLIKŠĶINĀT

Jūsu ierīcei pārtraucot funkcionēt, Jūs varat zaudēt naudu, personisko informāciju un pat savus saglabātos datus. Neuzķerieties!



KĀ TAS VAR NOTIKT?

PIKŠĶERĒŠANAS UZBRUKUMI: Uzbrucēji izmāna no lietotājiem personisku informāciju, uzdodoties par uzticamu iestādi. Viņi izplata savus viltus paziņojumus ar e-pastu, īsziņu vai sociālo tīklu starpniecību.

TĪMEKĻA PĀRLŪKOŠANA: Jūsu mobilā ierīce var tikt inficēta, vienkārši apmeklējot nedrošas tīmekļa vietnes.

FAILU LEJUPIELĀDE: E-pastā tiešā veidā var būt iegultas ļaunprātīgas saites vai pielikumi.

KĀDĒĻ TAS IR EFEKTĪVI

Mobilās ierīces **PASTĀVĪGI IR SAVIENOTAS** ar internetu.

Galvenais ierobežojums ir **IERĪCES EKRĀNA SAMAZINĀTAIS IZMĒRS.** Mobilās pārlūkprogrammas ataino URL ierobežotā ekrāna laukā, tāpēc ir grūti saredzēt, vai domēns ir pareizs.

LIETOTĀJA NEŠAUBĪGĀ UZTICĪBA mobilās ierīces personalizētajam raksturam.

KO ES VARU DARĪT?

Uzmanieties, ja saņemat īsziņu vai tālruņa zvanu no uzņēmuma, kas lūdz atklāt personisku informāciju. Jūs varat pārbaudīt ziņas/zvana autentiskumu, tiešā veidā piezvanot uzņēmumam pa oficiālo tālruņa numuru.

Pārlūkojot tīmekli savā mobilajā ierīcē, pārliecinieties, ka Jūsu savienojuma drošību garantē HTTPS. Jūs to vienmēr varat pārbaudīt URL sākumā.

Nekādā gadījumā neatveriet saiti/pielikumu nevēlamā e-pastā vai īsziņā. Nekavējoties izdzēsiet to.

Uzmanieties, ja nokļūstat vietnē, kuras teksts sastāv no gramatikas un pareizrakstības kļūdām vai kura tiek atainota zemā izšķirtspējā.

Ja iespējams, instalējiet mobilo ierīču drošības lietotni, kas brīdinās Jūs par jebkāda veida aizdomīgu darbību.

EUROPOL EC3 European Cybercrime Centre

LATVIJAS VALSTS POLICIJA

#MobileMalware