

Признаки опасности

Незнакомец выдает себя за работника банка/полицейского по телефону

Человек, выдавая себя за работника банка/полицейского по телефону, просит данные Вашей банковской карты или доступ к банковскому счету. Помните: настоящий работник банка/полицейский никогда не попросит такого!

Инвестиционное предложение

Вас направляют на веб-сайт, который «доказывает» доходность инвестиции – всё выглядит «как настоящее».

Незнакомец предлагает удивительную возможность увеличить капитал

Убедительным и бойким языком незнакомец по телефону или в интернете предлагает Вам фантастическую возможность увеличить капитал. Вы можете быть уверены, что если какое-либо предложение звучит слишком хорошо, чтобы быть правдой, то это и есть ложь.

Быстро-быстро-быстро!

По словам звонящего, нужно принимать решение/действовать сразу, иначе будут негативные последствия.

Тайная операция

Звонящий просит или даже приказывает сохранить в тайне всю деятельность, например, под предлогом, что это секретная операция.

Звонок с зарубежного номера

Вам звонят с зарубежного номера. Цель – выглядеть более важным и скрыть свое настоящее местоположение.

Просьба поделиться экраном компьютера

При общении в интернете/по телефону, Вам предлагается поделиться экраном вашего компьютера или загрузить программу (например, AnyDesk или TeamViewer). На самом деле, это дает мошеннику возможность удаленно контролировать Ваше устройство.

Знакомство в интернете

Неизвестный Вам человек хочет познакомиться с Вами, и начать дальнейшую беседу в мессенджере или по электронной почте. Позже просит финансовой помощи.

Ваш звонок переадресовывается другому учреждению

Вы получаете звонок якобы из банка или полиции, но во время разговора звонок перенаправляется в другое учреждение. Например, из одного банка в другой или в полицию.

Адрес веб-сайта отличается от оригинала

В адресной строке веб-сайта отличный от знакомого адрес: к нему добавлены буквы и цифры, или адрес вообще другой.

Полученная ссылка

Вам приходит ссылка по электронной почте или SMS, через которую запрашиваются данные банковской карты или вход в интернет-банк.

Отправленные документы некорректны

Вам отправлен документ, дизайн и текст которого некорректны.

Запрашиваются большие суммы в качестве платы за услуги

Чтобы получить услугу или продукт, Вы должны заплатить различные суммы в виде платы за услуги, часто на счет частного лица в зарубежном банке.

Неграмотное использование языка

Мошеннические письма часто написаны на плохом эстонском, используются странные названия учреждений или должностей, необычные выражения, и неправильный порядок слов или падежные окончания. Иногда текст можно вообще не понять. Странный и необычный текст должен сразу вызвать подозрения.

При малейшем сомнении **прекратите общение с тем, кто спрашивает коды**. Если Вы подозреваете, что перевели деньги возможному мошеннику или поделились данными банковского счета или карты, немедленно сообщите об этом своему банку и свяжитесь с полицией **по номеру 112**.

Читай подробнее:
pettuseinfo.ee

Eesti
Pangaliit

Veendu, mida PIN-koodiga kinnitat!

Enne oma PIN-koodide sisestamist veendu alati, mida sa täpselt kinnitat – tegemist võib olla pettusega.



Kindlad ohumärgid

Võõras esineb telefonis pangatöötaja/politseinkuna

Inimene, kes esineb telefonis pangatöötaja/politseinkuna, küsib sinu pangakaardi andmeid või ligipääsu pangakontole. Pea meeles: pärks pangatöötaja/politsei ei küsi kunagi selliseid asju!

Investeeringispakkumine

Sind juhatatakse veeblehele, mis „töestab“ investeeringu kasumlikkust – kõik näeb välja „nagu päris“.

Tundmatu pakub imelist võimalust raha kasvatada

Veenva ja sorava jutuga tundmatu pakub sulle telefoni teel või internetis fantastilist võimalust raha kasvatada. Võid kindel olla, et kui mistahes pakkumine kõlab liiga hästi, et tõsi olla, siis see ei olegi tõsi.

Kiire-kiire-kiire!

Helistaja sõnul peab otsustama/tegutsema kohe, muidu järgnevad negatiivsed tagajärjed.

Salajane toiming

Helistaja palub või lausa käsib kogu tegevust kõigi eest salajas hoida, näiteks ettekäändel, et tegu on salaoperatsiooniga.

Helistatakse välismaa numbrilt

Sulle helistatakse välismaa numbrilt. Selle eesmärk on mõjuda tähtsamalt ja varjata oma tegelikku asukohta.

Arvutiekraani jagamine

Kui suhtlete internetis/telefonitsi, palutakse sul oma arvutiekraani jagada või mõni programm alla laadida (nt AnyDest või TeamViewer). Tegelikult annab see petturile võimaluse sinu seade distantsilt enda kontrolli alla saada.

Tundmatuga tutvumine internetis

Tundmatu isik soovib Sinuga tutvuda ja alustada edasist vestlust suhtlusäpis või e-kirja teel. Hiljem palub rahalist abi.

Sinu köne suunatakse otse teisele asutusele

Saad köne väidetavalts pangast või politseist, kuid köne ajal suunatakse köne teise asutusse. Näiteks ühest pangast teise või politseisse.

Veeblehe aadress erineb originaalist

Veeblehe aadressiribal on tavapärasest erinev aadress: sellele on lisandunud tähed ja numbrid või on aadress sootuks erinev.

Saabunud link

Sulle saabub e-kirja või SMS-iga klinkitav link, mille kaudu küsitatse pangakaardi andmeid või sisselogimist internetipanga.

Saadetud dokumendid ei ole korrektsed

Sulle saadetakse dokument, mille kujundus ja tekst ei ole korrektne.

Küsitatse suurtes summades teenustasused

Et saada käte teenust või toodet, pead maksma erinevaid summasid teenustasudeks, sageli välismaa panga eraisiku kontole.

Konarlik keelekasutus

Petukirjad on sageli konarlikus eesti keeles, kasutatakse kummalisi asutuste või ametinimetusi ja väljendeid, vale sõnajärje või käändelõpp. Kohati võib tekst olla suisa arusaamatu. Kummaline ja veider tekst peaks kohe kahtlusi tekitama.

Vähimagi kahtluse korral **lõpetata suhtlus PIN-koodide küsijaga**. Kui kahtlustad, et oled petturi raha üle kandnud, jaganud oma pangakonto või -kaardi andmeid või öelnud oma PIN-koodid, teavita sellest kohe oma panga ning võta ühendust politseiga **numbril 112**.

Loe lähemalt:
pettuseinfo.ee

Eesti
Pangaliit

Убедись, что подтверждаешь PIN-кодом!

Осторожно! Прежде чем вводить PIN-код, убедитесь, что именно Вы подтверждаете — это могут быть мошенники.



