Как да се предпазите от атаки чрез съобщения

В европейския месец на киберсигурността обръщаме внимание на най-честите видове измами, с които се сблъскваме.

Един от най-често срещаните начини за измама, използвани от киберпрестъпниците, е да ви подведат по имейл (често наричани фишинг) или чрез телефонно обаждане. С развитието на технологиите злосторниците продължават да се опитват да измислят нови методи, включително измами чрез съобщения като SMS, iMessage/Facetime, WhatsApp, Slack, Viber или Skype. Ето някои прости стъпки, чрез които да забележите и предотвратите тези често срещани атаки.

Как да разпознаете атаките чрез съобщения?

Атаките чрез съобщения, понякога наричани “смишинг” (игра на думи от “фишинг”), са такива, при които атакуващият използва SMS или други технологии за текстови съобщения, чрез които да се свърже с вас и да ви убеди да предприемете действие, което иначе не бихте направили. Вероятно искат да ви подлъжат да последвате (кликнете) опасна интернет връзка или да се обадите на телефонен номер, за да ви попитат за информация относно банкиране (банкови транзакции, банкови сметки, пароли, вкл. за достъп до онлайн и мобилно банкиране и др.). Точно както при традиционните фишинг имейл атаки, злосторниците често се възползват от емоции, за да ви накарат да действате. Причината атаките чрез съобщения да са толкова опасни е, че често те се усещат много по-неофициални или лични, което увеличава вероятността да станете жертва. Освен това, при атаките със съобщения има много по-малко информация и признаци, чрез които да забележите, че нещо не е наред. Когато получите съобщение, което изглежда странно или подозрително, запитайте се – това съобщение има ли смисъл, защо го получавам?

Кой са най-отличителните признаци на атака?

Винаги съобщенията създават чувство за спешност, при което някой се опитва да ви накара много бързо да предприемете действие. Ако получите подобно съобщение, задайте си следните въпроси:

- Искат ли ви в съобщението лична информация, пароли или друга информация, до която никой не би трябвало да имат достъп?
- Съобщението звучи ли твърде хубаво, за да е истина?
  Не, не сте спечелили от лотарията, особено ако никога не сте играли.
- Съобщение, което изглежда, че идва от колега, приятел или познат телефонен номер, но изказът е различен. Техният акаунт може да е компрометиран от престъпници или атакуващият се преструва, че е някой, когото познавате, за да ви убеди да действате.
- Ако получите съобщение, което предизвиква силна емоционална реакция, почакайте известно време и помислите преди да отговорите.

Понякога злосторниците дори комбинират имейл и съобщения в една атака. Така работят измамите с предплатени карти или ваучери. Атакуващият ви изпраща спешен имейл, преструвайки се на ваш приятел или колега, след което пита за телефонния ви номер. След това могат да изпратят множество съобщения, притискайки ви да купите предплатена карта/ваучер. Веднъж купена такава, атакуващите ви карат да я отворите и да им пратите снимка на активационните кодове.

Друга често срещана атака иска от вас да "погледнете" изпратено видео или снимка ("няма да повярваш!" или с др. акцент). Така се възползват от естественото ви любопитство. Ако съобщението изглежда, че идва от някого, когото познавате, добре е да се обадите на този човек по телефона, за да проверите автентичността му преди да предприемете действието, за което Ви подканват.

Ако получите съобщение от официална организация, което ви тревожи, свържете се директно с организацията. Например, ако получите съобщение от вашата банка, в което се твърди, че има проблем с банковата ви сметка или банковата ви карта, свържете се с банката директно като посетите официалния ѝ уебсайт, за да отправите запитване чрез него или чрез посочените в него данни за контакт – имейл и телефонни номера, или да се обадете директно на телефонния номер, изписан на гърба на картата.

Не забравяйте, че при атаки чрез съобщения най-добрата защита сте самите вие. Бъдете внимателни и не споделяйте личните си данни!