Предотвратяване на измами

ТЕНДЕНЦИИ И СЪВРЕМЕННИ ОПИТИ ЗА ИЗМАМИ:

I. Фалшиво писмо от контрагент, партньор или близък за промяна на неговите банкови сметки:

Възможно е да получите фалшиво електронно писмо от свой партньор, към когото извършвате регулярни плащания или преводи. Чрез писмото ще бъдете уведомени, че Вашият контрагент има нови банкови сметки, които следва да бъдат използвани за бъдещите разплащания с него. Имайте предвид, че това е опит за измама, целяща клиентът сам да нареди превод към сметката на измамника.
При получаване на информация за подмяна на данни на Вашите контрагенти (сметки, адрес, телефон и др.), винаги установявайте личен контакт с тях с цел потвърждение на промените от първо лице. Внимателно сравнявайте получения имейл с предходни мейли от същия кореспондент.
При подмяна на сметка за плащане по фактура, винаги се свързвайте с Вашия контрагент по канал, различен от имейл, с искане за потвърждение на реквизитите по плащането. При покупка на стоки по обяви в интернет, проверявайте детайлно сайта на търговеца и публикацията.

II. Фалшиво телефонно обаждане или имейл:

Тази схема на измама включва телефонно обаждане или имейл от лице, представящо се от името на реномирана институция (Банката, куриерска фирма, интернет доставчик, различни държавни институции, дружества за комунални услуги или др.). В разговора или писмото, под предтекст оказване на съдействие – корекция на сгрешен превод, очаквана пратка или др., се изисква от Вас да предоставите получения SMS код или друга важна информация. Имайте предвид, че институциите не изискват лична и банкова информация. Предвид същото, никога не предоставяйте SMS кодове, пароли за достъп, номера на банкови карти и др. на лица по телефон или в отговор на имейл. Запишете телефонния номер, от който се обажда лицето или препратете писмото на Банката и се свържете с денонощния ѝ център за контакт с клиенти.
При получаване на мейли от институции, както е посочено по-горе, с информация, че картата Ви е блокирана, че се иска актуализация на профила Ви или др., с инструкции за връщане на достъпа чрез следване на линк и предоставяне на лични данни, знайте, че това е фишинг атака, която цели да събере конфиденциална информация от Вас, с която да се злоупотреби. Ако към подобен мейл има прикачени архивирани файлове, също не ги отваряйте, защото могат да заразят устройството Ви.
Не инсталирайте приложения за отдалечен достъп на техниките си, чрез които създавате и изпращате платежни нареждания чрез електронните канали. Следвайте препоръките за сигурност на производителя, както и на Банката.

III. Фалшиви оферти за кредитиране през социалните мрежи:

Тази схема включва получаване на оферти за кредитни продукти от фалшиви страници на Банката или други институции в социалните мрежи и по канали като Viber, WhatsApp и други подобни. Ако получите подобна оферта, проявявайте бдителност и не предоставяйте личните си данни и данни за банковите си карти, както и съпътстващите еднократна парола или активационен код за конкретна услуга. Не предоставяйте снимки (копия) на лични и банкови карти и не изпращайте пластиките на банковите си карти на трети лица.
Бъдете особено внимателни, когато от Вас се иска да внасяте определени суми под формата на такси, комисионни и други основания по сметки на физически лица в банкови институции във връзка с кандидатстване за финансиране.

IV. Измами с банкови карти:

Използването на дебитни и кредитни карти е част от нашето ежедневие и все по-често извършваме плащания при онлайн търговци с тях. В тази връзка, интересът на лицата, занимаващи се с измамни схеми е изключително висок точно в тази сфера. В тази връзка, Ви препоръчваме да бъдете бдителни и при покупки от нови и/или непознати за Вас сайтове и интернет търговци, които предлагат атрактивни цени за стоки и абонаменти. Внимавайте дали наистина пазарувате от сайта на истинския онлайн търговец, а не такъв, който много прилича на него и го копира.
Запознайте се внимателно и с условията на доставка, процедурата за връщане на стоката и правото на отказ. Проверете наличната информация за търговеца, както и за мнения и препоръки от Ваши близки.
Избирайте сайтове, които са включени в програмите за сигурни плащания с банкови карти на Visa и Mastercard - Verified by VISA и MasterCard Secure Code. Ако сайтът не ги поддържа, то проверете дали е защитен – погледнете за икона на ключ или катинар, както и за изписване на https:// преди адреса на сайта.
Пазете картовите си данни, не ги предоставяйте на други лица и не ги оставяйте без надзор на обществени места. Не съхранявайте ПИН кода си заедно с картата на хартиен и друг носител.
Бъдете бдителни не само при покупки, но и при продажби от Ваша страна в различните платформи. Не следвайте линкове, изпратени до Вас от трети лица и не въвеждайте данните за Вашите банкови карти преди да сте се убедили в коректността на насрещната страна. Не предоставяйте на трети лица получената от Вас динамична парола за потвърждаване на дадено онлайн плащане с карта в телефонен разговор или чат приложение. Същата е уникална и е предназначена само за лично ползване от Вас при покупки с карта при интернет търговци.

При съмнения за измама, загуба или кражба на карта, своевременно се свържете с Център за контакт с клиенти на телефон 0700 1 84 84 (кратък номер 1 84 84) или на имейл: CallCentre@UniCreditGroup.bg.

V. Инвестиционни измами

При този тип схеми, измамниците се опитват да подмамят хората да инвестират средства, като им обещават висока доходност и нисък риск. Те може да искат да инвестирате пари в акции, облигации, стоки, валута и др. Измамник може да Ви излъже или да Ви даде фалшива информация за реална инвестиция.
Често лицата, които се стремят да Ви въведат в заблуда, се представят за професионалисти, създавайки си фалшиви профили в социалните мрежи като например в LinkedIn. Обикновено измамникът си създава профил и насочва потребителя към легитимна инвестиционна платформа, но след като спечели доверието му в продължение на няколко месеца, му казва да премести инвестицията на сайт, контролиран от самия него. В резултат на това, източва средствата от сметката му.
За да се предпазите от този тип измамна схема, следва да проверявате дали компанията, която Ви предлага инвестиционни услуги е лицензирана. Проверка за лиценз може да се осъществи на сайта на Комисията за финансов надзор. Също така е важно да не се доверявате на лица, които се свързват с Вас през социалните мрежи и Ви обещават помощ при инвестиране, нереалистични печалби и нулев риск.

VI. Телефонни измами

Налични са опити за телефонни измами от международни телефони, които се изразяват с еднократно позвъняване. Имайте предвид, че този вид обаждания целят отдалечено да се атакуват Вашите телефони с оглед да се установи контрол върху телефона Ви и да се откраднe лична и финансова информация, записана на телефонните Ви устройства. Тези злоумишлени действия са възможни, ако отговорите или върнете обаждане на номера, който Ви е търсил.
В тази връзка, приемайте и връщайте обаждания само на познати от Вас телефонни номера, не отговаряйте и не връщайте обаждане на международни номера и не следвайте инструкции за избиране на номер с нетипични символи. Ако сте попаднали на подобно обаждане и сте отговорили или върнали разговор, сменете паролите за достъп на всички акаунти, които използвате през телефона си. Ако услугите, които използвате позволяват включване на по-високо ниво за защита (допълнително потвърждаване, втора парола), ги активирайте. Проверете дали само Вие сте администратор на телефона и ако има процес/администратор, който е различен от познатите Ви, го премахнете.

В случай на най-малкото съмнение за злоупотреба с личните Ви данни, се свържете незабавно с банката на номер 0700 1 84 84 или кратък номер 1 84 84.

VII. Други типове измами

Много често измамниците си създават фалшива онлайн самоличност, целяща установяване на взаимоотношения и печелене на доверието на жертвата. Престъпниците застават зад фалшива самоличност в различни сайтове за запознанства, в социалните мрежи и по мейл. Намерението на измамника е да установи връзка възможно най-бързо, да се хареса на жертвата и да спечели доверие. Измамниците могат да предложат брак и да правят планове за лична среща, но това никога няма да се случи. В крайна сметка те ще поискат пари. Престъпниците често казват, че са в чужбина, което улеснява избягването на лична среща и е по-правдоподобно, когато искат пари за спешна медицинска помощ, за закупуване на самолетни билети или неочаквани такси и разходи. Знайте, че не следва да изпращате пари на подобни лица, с които комуникирате във виртуалното пространство или по телефон, нито да предоставяте лични и банкови данни.

Съществуват и измами, при които жертвата получава имейл или писмо от името на банка, адвокат или др., в което се съобщава, че е наследник на далечен роднина, за когото най-вероятно никога не е чувала. При този тип измами престъпниците твърдят, че предполагаемото наследство е труднодостъпно, поради правителствени разпоредби, данъци или банкови ограничения в страната, където се съхраняват парите, и че трябва да се заплати определена сума и/или да се предоставят лични данни, за да ги се изплати наследството. Не забравяйте, че няма схеми за бързо забогатяване: ако звучи твърде добре, за да е истина, вероятно е така.

Повече информация как да се предпазите от измами, както и съвети за киберсигурност, може да откриете на сайта на банката:
https://www.unicreditbulbank.bg/bg/individualni-klienti/bankirane/saveti-za-kibersigurnost/.