УниКредит Булбанк полага професионални грижи за защита на своите клиенти, като използва най-съвременните световни практики и технологии в областта на интернет сигурността и алтернативните канали за банкиране.

Не по-малко важно за Вашата сигурност, обаче, е поведението Ви в интернет пространството и използваните от Вас средства за защита на Вашия компютър и устройства за интернет достъп.

Препоръки за сигурност при работа с алтернативни канали за банкиране

- Моят компютър/устройство разполага с антивирусен софтуер, който се актуализира редовно
- Антивирусната ми програма има функция за разпознаване на зловреден софтуер, spyware и програми от типа „троянски кон“
- Сканирам редовно своя компютър за вируси
- Сменям паролата си за алтернативни канали за банкиране поне веднъж в месеца
- Браузърът, който използвам за банкиране, е настроен на най-високото ниво на защита на данните
- Използвам последна версия системен софтуер, уеб браузер, операционна система и firewall
- При вход в алтернативните канали за банкиране, винаги се уверявам в автентичността на страницата, като проверявам, дали адресният бар е оцветен в зелено и адресът на страницата започва с https://
- Пазя в тайна и не запаметявам в интернет браузъра моето потребителско име и парола
- Не инсталирам програми с неясен произход и не следвам линкове в съмнителни съобщения и имейли на компютъра, от който банкирам
- Свалям софтуер на моя телефон/ мобилно устройство единствено от официалните магазини за приложения – App Store, Google Play
- Не държа постоянно включен в компютъра моя Квалифициран Електронен Подпис (*в случай че използвам такъв*), когато не работя с него

Ако отговаряте на всички въпроси с „Да“, Вие бихте могли да сте спокойни, че сте направили всичко необходимо за Вашата сигурност при използване на алтернативни канали за интернет банкиране

От какво трябва да се пазим – типове онлайн измами

С нарастване на използването на интернет в световен мащаб се увеличават действията на криминалния контингент, целящи различни форми на измама спрямо потребителите в глобалната мрежа, включително към клиентите, използващи алтернативни канали за интернет банкиране.

За нас, като Банка с приоритет върху сигурността на нашите клиенти, е важно да Ви запознаем с действащите измамни схеми в сферата на алтернативните канали за интернет банкиране, така че при евентуалната им проява да ги идентифицирате и своевременно да се предпазите от тях.

Актуални трикове и опити за измама на кибер престъпниците

Вариант 1

ФАЛШИВО ТЕЛЕФОННО ОБАЖДАНЕ ИЛИ ИМЕЙЛ

Описание: *Тази схема на измама включва телефонно обаждане или имейл от лице, представящо се от името на реномирана институция (Банката, куриерска фирма, интернет доставчик 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 от Вас SMS код* или друга важна информация.

ПОМНЕТЕ! Това е опит за измама, целяща клиентът сам да разкрие личната банкова информация и получения от него SMS код за потвърждение.

Необходими действия: Никога не предоставяйте лична банкова информация (SMS кодове, пароли за достъп, номера на банкови карти) на други 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 й център за контакт с клиенти.

Вариант 2

ФАЛШИВО ПИСМО ОТ КОНТРАГЕНТ, ПАРТНЬОР ИЛИ БЛИЗЪК ЗА ПРОМЯНА НА НЕГОВИТЕ БАНКОВИ СМЕТКИ

Описание: *Възможно е да получите фалшиво писмо от свой партньор, към който извършвате регулярни плащания или преводи. Чрез писмото ще бъдете уведомен, че Вашият контрагент има нови банкови сметки, които следва да бъдат използвани за бъдещите разплащания с него.*

ПОМНЕТЕ! Това е опит за измама, целяща клиентът сам да нареди превод към сметката на измамника.

Необходими действия: При получаване на информация за промяна на данни на Вашите контрагенти (сметки, адрес, телефон и др.), винаги установявайте личен контакт с тях с цел потвърждение на промените от първо лице.

От какво трябва да се пазим – типове онлайн измами

Актуални трикове и опити за измама на кибер престъпниците

Вариант 3

ФАЛШИВО СЪОБЩЕНИЕ, ПРИКАНВАЩО СЛЕДВАНЕ НА ПРОЦЕДУРА ЗА ПРОВЕРКА

Описание: *При опит за вход в алтернативните канали за интернет банкиране се визуализира фалшив екран, наподобяващ Булбанк Онлайн. На него, под претекст предотвратяване на кражба на лични данни, потребителя бива приканван да следва процедура за генериране и изпращане на SMS парола/ код с цел потвърждение и възобновяване на неговия нормален достъп.*

ПОМНЕТЕ! Това е опит за измама, целяща прихващане на SMS парола! Bulbank Online не изисква въвеждане на SMS парола при вход в услугата. SMS код се генерира единствено в резултат от извършена от потребителя активна операция в системата – превод или др.

Причина за проява: Компютърът е заразен с вирус, който манипулира интернет браузъра и визуализира фалшив екран на потребителя. Обикновено, посредством вирус, хакерът предварително вече е придобил пълен контрол върху компютъра на жертвата.

Необходими действия: В никакъв случай не следвайте описаната процедура и се свържете незабавно с Банката на телефона на денонощния център за контакт с клиенти.

Вариант 4

ФАЛШИВО СЪОБЩЕНИЕ, ИЗИСКВАЩО ВЪВЕЖДАНЕ НА ДАННИ ЗА МОБИЛЕН ТЕЛЕФОН - ОПЕРАЦИОННАТА СИСТЕМА И ТЕЛЕФОНЕН НОМЕР

Описание: *След влизане в алтернативните канали за интернет банкиране се визуализира фалшив екран, наподобяващ Булбанк Онлайн. На него, под предтекст допълнителна защита на мобилния телефон на клиента от „вредоносен софтуер“, се изисква потре-бителят да следва стъпки за инсталиране на мобилна антивирусна програма, чрез въвеждане на данни за операционна система, номер на телефон и др.*

ПОМНЕТЕ! Това е опит за измама, целяща инсталирането на хакерска програма на телефона, която да пренасочва получените от Банката съобщения към телефонния номер на измамника.

Причина за проява: Компютърът е заразен с вирус, който манипулира интернет браузъра и визуализира фалшив екран на потребителя. Обикновено, посредством вируса, хакерът предварително вече е придобил пълен контрол върху компютъра на жертвата.

Необходими действия: В никакъв случай не следвайте описаната процедура и получения на телефона линк за сваляне на програмата за защита. Необходимо е да се свържете незабавно с денонощния център за контакт с клиенти на Банката.

В случай на необходимост от съдействие, информация или съмнения за неоторизиран достъп до Вашия компютър се свържете незабавно с Банката на телефон 0700 1 84 84 или кратък номер *1 8484 от Вашия мобилен телефон.