UniCredit Bulbank

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

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

Препоръки за сигурност

Изберете една от категориите, за да научите повече

Препоръки
Какво трябва да знам и правя за моята сигурност?

Чек лист
Спазвам ли необходимите мерки за сигурност?

Предотвратяване на измами
Как да се пазя от съвременните опити за измама от кибер престъпниците?

Още за сигурността
Какво още трябва да знам за своята сигурност?

UniCredit Bulbank

Препоръки за сигурност

КАКВО ТРЯБВА ДА ЗНАМ И ПРАВЯ ЗА МОЯТА СИГУРНОСТ?

Информационната сигурност е от съществено значение за онлайн и мобилното банкиране. УниКредит Булбанк полага професионални грижи за опазване на сигурността на компютърната си мрежа, част от която е и сайтът на Булбанк Онлайн. Не по-малко важни за сигурността на използваното от Вас онлайн банкиране са и предприетите от Ваша страна мерки – на Вашите компютри, компютърни мрежи и интернет достъп.

УниКредит Булбанк разрешава достъп до Булбанк Онлайн чрез обичайните средства за идентификация – потребителско име и парола, а за активни операции – чрез допълнително средство за оторизация (КЕП, цифров сертификат, мобилен токен). Ако сигурността на Вашия компютър бъде компрометирана, злонамерени лица могат да получат достъп до Вашите средства за идентификация, а чрез тях – до онлайн банкирането от Ваше име. По такъв начин може да бъде получен достъп до банкова информация по отношение на Вашите сметки, както и до паричните средства по тях.

Вашата отговорност като потребител на онлайн и мобилното банкиране е да опазвате персоналните си средства за индентификация съгласно изискванията в Общите условия за услугите за електронно банкиране Булбанк Онлайн и Булбанк Мобайл.

- **Не използвайте публични компютри и софтуер с неясен произход.**
- **Проверявайте изпращача на имейл съобщения и не предоставяйте конфиденциална информация.**
- **Проверявайте индикациите за сигурност на уеб-сайтовете.**
- **Избягвайте запаметяване на потребителски имена и пароли в уеб-браузъра и компютъра Ви.**
- **Използвайте лицензиран антивирусен софтуер, анти-спайуеър и firewall. Препоръчително е те да бъдат поддържани от специалист.**
- **При предоставяне на физически достъп до компютъра Ви на трети лица, изтривайте от него всички средства за идентификация и оторизация.**
- **Обновявайте използвания от Вас софтуер, уеб браузър и операционна система, следвайте препоръките за сигурност на производителя.**

Булбанк Онлайн

- **Не разкривайте на никого своето потребителско име и парола, сменяйте ги често. Включително не предоставяйте SMS пароли и кодове от М-токен на трети лица.**
- **Проверявайте достъпа до Булбанк Онлайн от Ваше име, винаги използвайте „Изход” след използването на сайта.**
- **Препоръчително е да използвате Квалифициран Електронен Подпис или цифров сертификат върху хардуерно криптографско устройство.**
- **За корпоративни клиенти – преценете възможността за комбиниран подпис.**
- **При съмнение за неоторизиран достъп от Ваше име до Булбанк Онлайн веднага информирайте УниКредит Булбанк.**

Булбанк Мобайл

- **Заключвайте винаги телефона си и определете ПИН / парола за достъп. Не записвайте пароли за достъп на телефона си, не споделяйте достъпа си до телефона, както и самия телефон с трети лица.**
- **Телефонът трябва да е актуализиран до последна налична версия на операционната система.**
- **При липса на комуникационни услуги с номера Ви, моля веднага изискайте от доставчика на мобилния Ви оператор статус и при деклариране за смяна или преиздаване на SIM карта изискайте незабавно блокиране. Веднага информирайте УниКредит Булбанк и изискайте блокиране на мобилното банкиране от банката.**
- **Не ползвайте програми, предоставящи отдалечен достъп до Вашия телефон.**
- **Инсталирайте приложения на вашия телефон само от официалните магазини за приложения: AppStore / Google Play.**

Чек лист за сигурност

Спазвам ли необходимите мерки за сигурност?

UniCredit Bulbank

Чек лист за сигурност

СПАЗВАМ ЛИ НЕОБХОДИМИТЕ МЕРКИ ЗА СИГУРНОСТ?

Прегледайте посочените мерки за сигурност и проверете дали отговаряте на всяка от тях.

При покриване на всички въпроси с положителен отговор „**ДА**“, Вие бихте могли да сте спокойни, че сте направили всичко необходимо за Вашата сигурност при използване на електронните канали за интернет и мобилно 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 ЕЛЕКТРОННИТЕ 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 ЕЛЕКТРОННИТЕ 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, ТЕЛЕФОНА И КОМПЮТЪРА 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 УНИВЕРСАЛЕН ЕЛЕКТРОНЕН ПОДПИС (В СЛУЧАЙ ЧЕ ИЗПОЛЗВАМ ТАКЪВ), КОГАТО НЕ РАБОТЯ С НЕГО

UniCredit Bulbank

Предотвратяване на измами

КАК ДА СЕ ПАЗЯ ОТ СЪВРЕМЕННИТЕ ОПИТИ ЗА ИЗМАМА ОТ КИБЕР ПРЕСТЪПНИЦИТЕ?

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 електронни 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 електроните канали за интернет и мобилно 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

- Фалшиво съобщение, изискващо въвеждане на данни за мобилен телефон – операционна система и телефонен номер
- Фалшиво телефонно обаждане или имейл
- Фалшиво писмо от контрагент / партньор / близък за промяна на неговите банкови сметки

Фалшиво съобщение, изискващо въвеждане на данни за мобилен телефон - операционната система и телефонен номер

ОПИСАНИЕ

След влизане в електроните 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 потребителят 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.

Предотвратяване на измами

КАК ДА СЕ ПАЗЯ ОТ СЪВРЕМЕННИТЕ ОПИТИ ЗА ИЗМАМА
ОТ КИБЕР ПРЕСТЪПНИЦИТЕ?

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.

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.

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

UniCredit Bulbank

Още за сигурността

КАКВО ОЩЕ ТРЯБВА ДА ЗНАМ ЗА СВОЯТА СИГУРНОСТ?

Тук ще намерите мерки за обща компютърна сигурност, както и мерки, специфични за онлайн банкирането. Придържането към тях в голяма степен ще повиши сигурността на използването на онлайн банкирането от Вас и, по този начин – на информацията и средствата по Вашите банкови сметки.

ДОСТЪП

- **Избягвайте използването на Булбанк Онлайн от публично достъпни компютри, както и от такива с неконтролиран достъп**
- **Не разкривайте на никого и под никакъв предлог потребителското си име или парола за достъп до Булбанк Онлайн – те са лични**
  При необходимост от достъп на служител на фирмата Ви или на член от семейството, Вие като титуляр на сметките може да заявите отделен достъп за него – от Банката ще му бъдат предоставени ново потребителско име и парола със заявеното от Вас ниво на достъп – само за информация, за нареждания или с определен лимит.
- **Никога не пазете на материален носител потребителското си име и парола.**
- **При съмнение, че някой използва Вашето потребителско име и парола, незабавно ги сменете чрез предоставените за това средства на сайта на Булбанк Онлайн! При невъзможност се свържете с Банката и и изискайте блокирне на достъпите ви.**
- **Ако скоро не сте променяли паролата си, отделете малко време и извършете това действие**
  Използвайте комбинация от букви, цифри и символи. Променяйте паролата си за достъп по-често. По този начин намалявате вероятността паролата Ви да бъде лесно разгадана.
- **Препоръчително е да избягвате т. н. “автоматично запаметяване“ на идентификационните Ви данни или пароли в паметта на браузъра, на диска на използвания от Вас персонален компютър или телефона Ви**

ВНИМАНИЕ!
Идентификационните кодове (кодове за достъп и PIN), използвани за достъп до нашите банкови услуги чрез Интернет, не трябва да се “записват” в паметта на браузъра Ви или на диска на персоналния Ви компютър. Добре е да проверите дали функцията “автоматично попълване” на браузъра не е активирана.

Инструкция за деактивиране:

INTERNET EXPLORER:

1. *Изберете меню “Tools” >> “Internet Options”.*
2. *От частта “Content”, в секцията “Personal information” , изберете “Auto Complete”.*
3. *Премахнете отметката на „Usernames and passwords on forms”, ако има такава, кликнете върху бутоните “Clear forms” и “Clear passwords”.*
4. *Потвърдете с OK и затворете отворените менюта.*

MOZILLA FIREFOX:

1. *Изберете меню “Tools - Options” >> “Security”.*
2. *От частта “Passwords”, премахнете отметката от “Remember passwords for sites”, ако има такава.*
3. *Потвърдете с OK и затворете отворените менюта.*

Още за сигурността

КАКВО ОЩЕ ТРЯБВА ДА ЗНАМ ЗА СВОЯТА СИГУРНОСТ?

ЦИФРОВ СЕРТИФИКАТ

- **Пазете Вашия цифров сертификат**
  Ако се наложи да пренасяте цифровия си сертификат до друг компютър, винаги го изтривайте след употреба – като от браузъра, така и файла, чрез който е пренесен. Пренасянето на сертификата е желателно да става лично от потребителя, на когото е издаден. Защитавайте сертификата с парола при пренасянето му.
- **Препоръчително е използването на хардуерно криптографско устройство за съхранение на цифровия Ви сертификат**
  Цифрови сертификати, съхранявани в браузъра, биха могли да бъдат експортирани от там и използвани от злонамерени лица за създаване и подписване на платежни нареждания от Ваше име. Сертификатът от хардуерното криптографско устройство НЕ може да бъде експортиран – той е използваем единствено чрез устройството, плюс необходимия PIN за него.
- **Препоръчително е използването на Универсален Електронен Подпис (УЕП)**
  Универсален електронен подпис представлява персонален цифров сертификат върху хардуерно криптографско устройство и означава усъвършенстван електронен подпис, който е създаден от устройство за създаване на универсален електронен подпис и се основава на квалифицирано удостоверение за електронни подписи. Издава се от доставчик на удостоверителни услуги съгласно Закона за електронния документ и електронните удостоверителни услуги.

ИНТЕРНЕТ ПРОСТРАНСТВО

- **Предлаганите сайтове, особено ако изискват конфиденциална информация или парола, не трябва да се посещават дори и за кратки периоди**
  Посоченият в имейла линк може да не е този, който изглежда в действителност, а получените файлове в повечето от случаите крият рискове. Не следвайте линковете в получените имейли, тъй като те могат да Ви заведат до ”опасен” или “фалшив” сайт, който трудно може да бъде различен от оригиналния. Дори в полето на адреса в браузъра да се вижда коректният адрес, не се доверявайте - визуализираният уеб-адрес може да е бил променен от измамник. УниКредит Булбанк не изисква от клиентите си да въвеждат лични идентификационни данни или друга конфиденциална информация в официалния си уеб сайт.
- **По време на сърфиране в Интернет избягвайте да давате финансова информация и особено конфиденциални данни (като парола или номера на кредитни / дебитни карти) в който и да било Интернет сайт без предварително да сте проверили сигурността на комуникационния протокол и автентичността на уеб сайта**
  Имате възможност за проверка на комуникационния протокол: 1) “HTTPS://“ в началото на уеб адреса и 2) икона в жълт цвят, изобразяваща “заключен катинар” (който показва SSL протокол) в полето за състояние на браузъра. Като част от Групата UniCredit, УниКредит Булбанк използва този сигурен протокол имащ за цел да предпазва и гарантира конфиденциалността на информацията, която Вие въвеждате по време на използването на Интернет банковите услуги. За проверка автентичността на сайта кликнете два пъти върху споменатата по-горе икона с форма на заключен катинар и вижте информацията от издателя на сертификата на уеб сайта.

UniCredit Bulbank

Още за сигурността

КАКВО ОЩЕ ТРЯБВА ДА ЗНАМ ЗА СВОЯТА СИГУРНОСТ?

ЕЛЕКТРОННА ПОЩА И СЪОБЩЕНИЯ

- **Правете проверка на подателя на получени от Вас имейл съобщения.**
  Имейлите, целящи измама, е възможно да се разпознаят по следното:
  - съдържат съобщения с искане за лични, конфиденциални данни, като причините не са конкретно посочени (например: изтичане срока на кодовете, загуба на кодове, технически проблеми или такива, свързани със сигурността)
  - често те използват „заплашителен" тон; съдържат например заплахи за прекратяване на услугата, в случай че не изпратите отговор - такива никога не се изпращат чрез съобщенията на УниКредит Булбанк;
  - не се посочва крайният срок за изпращане на исканата информация.
- **При получаване на съмнителни имейл съобщения:**
  Не използвайте посочените в тях линкове (линкът представлява препратка към дадена интернет страница (сайт), зареждането на която става с кликване на левия бутон на мишката върху линка). Не отваряйте приложените към имейла файлове.
- **Препоръчително е използването на универсален електронен подпис, чрез които се удостоверява автентичността на подателя и съдържанието на мейла.**
  Подписването на мейли с универсален електронен подпис удостоверява автентичността на податели, като по този начин могат да се намалят рисковете от получаване на изпратени с незаконни цели имейли.
- **При получаването на имейли с цел измама е необходимо да сигнализирате по най-бързия начин прокуратурата или полицията, както и самата Банка**
  Не отговаряйте, а веднага информирайте Банката чрез центъра за обаждания или като посетите обслужващия Ви филиал. Сигнализирането на компетентните власти за случаи, които считате за престъпления, позволява на същите незабавно да се намесят, а на Банката – да предприеме ответни защитни мерки, за да предпази клиентите си.
- **Не се доверявайте при неочаквани промени в начина, по който се изисква от Вас да въвеждате Вашите кодове за достъп до Интернет услугата**
  В случай на неочаквана промяна относно начина, по който попълвате Вашите кодове за достъп до Интернет услугата, за която не сте уведомени, молим да се свържете с Банката чрез центъра за обаждания или като посетите обслужващия Ви филиал.
- **УниКредит Булбанк, като част от групата на UniCredit, не изисква кодове, пароли за достъп или друга конфиденциална информация по електронната поща (имейл).**
  Не се доверявайте на имейл, в който се изискват конфиденциални данни, дори да е получен от познати податели. При никакви обстоятелства УниКредит Булбанк не изисква от своите клиенти чрез имейл пароли, потребителски идентификатор, кодове за достъп до услуги (например Булбанк Онлайн), PIN-кодове, номера на банкови карти или друга конфиденциална информация.

UniCredit Bulbank

Още за сигурността

КАКВО ОЩЕ ТРЯБВА ДА ЗНАМ ЗА СВОЯТА СИГУРНОСТ?

ЗАЩИТА

- **Препоръчително е използването на антивирусен софтуер**
  Имейлите или уеб сайтовете, които целят измама, могат да съдържат и опасни програми, които са създадени с цел да прихванат и препратят конфиденциални лични данни към компютъра на злонамерено лице. Антивирусните пакети са в състояние да открият и алармират за наличието на такива опасни програми. Препоръчително е използването на антивирусна програма да е от лицензиран или свободен доставчик, но никога от копие или компрометиран източник. Препоръчително е използваната антивирусна програма да бъде поддържана от специалист.

- **Препоръчително е използването и поддържането на актуален персонален и корпоративен Firewall при наличието му**
  Спайуеър представляват компютърни програми, които следят потребителските действия, записват въведена от потребителя информация и я предават на злонамерени лица. Могат да бъдат инсталирани на Вашия компютър от злонамерено създаден софтуер, уеб сайт или имейл. Съществуват комбинирани решения антивирусни / анти-спайуеър / firewall решения. Препоръчително е използваното решение да бъде поддържано от специалист.

- **Препоръчваме актуализиране поне веднъж на тримесечие операционната система и всички използвани програми**
  Фирмите-производители на софтуер, операционни системи и уеб браузъри периодично предоставят онлайн актуализации на същите, които могат да бъдат безплатно заредени (т. н. patch) и като подобрения увеличават и нивото на сигурност. В уеб сайтовете на тези фирми можете да проверите дали Вашият браузър е актуализиран и, в случай че не е, да инсталирате актуалните patch.
  Поддържането на актуална операционна система, браузър, електронна поща и ползван софтуер, като цяло намалява т. н. уязвимост на приложенията, от която обикновено се възползват информационните престъпници. Следвайте инструкциите за сигурност, давани от производителя на операционната система и друг софтуер, който използвате!

- **Не инсталирайте и не използвайте софтуер със съмнителен и недоказан произход**

- **Проверявайте достъпа до Булбанк Онлайн от Ваше име чрез средствата, предоставени на уеб сайта**

- **При необходимост от поддръжка от страна на УниКредит Булбанк, по възможност използвайте свободни съобщения на сайта на Булбанк Онлайн, а не имейл адреса за поддръжка**

- **При ремонт на Вашия компютър или предоставянето по други причини на физически достъп до него на трети лица, включително и обслужващите компютъра Ви специалисти:**
  Моля експортирайте, защитете с парола, съхранете на външен носител и пазете на сигурно място Вашия цифров сертификат, като след това го изтриете от браузъра, с който работите. За тази цел, следвайте инструкциите на производителя на Вашия браузър или тези в Булбанк Онлайн.

- **За корпоративни клиенти е удачно да прецените използването на комбиниран подпис на платежните нареждания. Тази възможност се предоставя от Булбанк Онлайн и може да бъде заявена и предоставена според Вашите изисквания без допълнително заплащане**

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

UniCredit Bulbank