Как мога да направя онлайн банкирането си сигурно?

ПроКредит Банк е ангажирана с предприемане на редица мерки, за да защити Вашите онлайн плащания и да запази целостта на данните във Вашия банков акаунт. За да постигнем това, ние използваме последна версия софтуер за сигурност и прилагаме различни процедури за безопасност. Въпреки това, Ви молим да имате предвид, че Интернет и електронната Ви поща може да бъдат използвани като средство за незаконна дейност. Ето защо, препоръчваме да предприемете няколко прости предпазни мерки, които ще направят онлайн банкирането Ви по-сигурно.

Съвети за онлайн сигурност

Знаете ли с кого си имате работа?

Винаги влизайте в портала за онлайн банкиране като въвеждате Интернет адреса на банката в полето на Вашия уеб браузър https://probanking.procreditbank.bg/.

Никога не посещавайте сайт и не въвеждайте личните си данни, като последвате линк, посочен в имейл съобщение, за което не сте сигурни, че е легитимно.
Ако се съмнявате, моля свържете се с ПроКредит Банк на тел. **(+359) 2 81 35 100.**

Пазете паролите си

Винаги бъдете внимателни с неоторизирани имейл съобщения или телефонни обаждания, които искат от Вас да разкриете лична информация или номерата на банковите ви карти. ПроКредит Банк или полицията никога не би се свързала с Вас, с искане да предоставите лични данни или да разкриете информация за използваните от Вас пароли. Пазете тази информация в тайна. Бъдете предпазливи при предоставяне на личните Ви данни на някого, особено ако не го познавате.

Грижете се за сигурността на персоналния си компютър

Използвайте последните версии на антивирусните програми и персонални защитни стени (firewall). Винаги използвайте последна версия на използвания от Вас уеб браузър, включваща всички актуални обновявания към момента. Бъдете изключително предпазливи, ако използвате Интернет на обществени места – в кафенета, библиотеки или какъвто и да е чужд персонален компютър, върху който нямате контрол.

Пазете парите си!

Не се подлъгвайте по искрено звучащи имейл съобщения, които Ви предлагат възможност да изкарате лесни пари. Това, което изглежда прекалено хубаво, е много вероятно да не е истина. Бъдете изключително внимателни с непоискани имейл съобщения от други държави, тъй като е много по-трудно да проверите дали са изпратени от хората, за които се представят подателите.

За повече информация посетете специализирани уеб страници като:

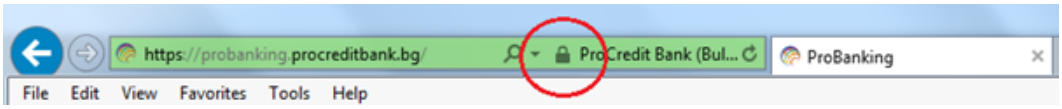
http://www.staysafeonline.org/stay-safe-online

Допълнителни съвети за онлайн сигурност

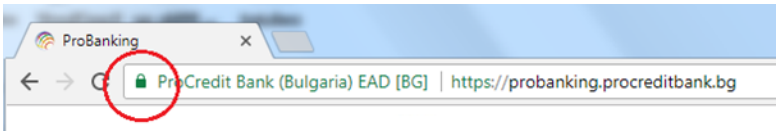
Знайте с кого си имате работа

- Винаги използвайте **сигурната услуга на ПроКредит Банк за електронно банкиране.** Преди да влезнете в сайта на банката, проверете за наличието на заключен катинар или цял ключ долу вдясно в прозореца на браузъра Ви. Началното изписване на Интернет адреса на банката ще се промени от “http” на “https” когато се осъществи безопасна връзка.
- Може да проверите Сертификата за сигурност на уеб сайта на ПроКредит Банк, като натиснете катинара, който се появява в браузъра Ви.

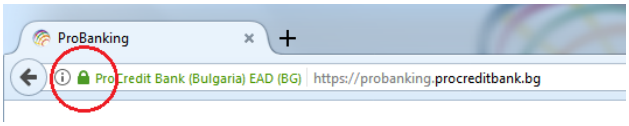
Internet Explorer:



Chrome:



Mozila:



Пазете паролата си

- Винаги запомняйте паролите си или друга информация, свързана с Вашата сигурност и възможно най-бързо унищожавайте документите, съдържащи такава информация.
- Бъдете отговорни при опазване тайната на Вашата парола или друга информация, свързана с Вашата сигурност – никога не я разкривайте на членове на семейството, приятели и др.
- Обаждайки се в банката, трябва да сте запознати каква информация ще бъде поискана от Вас. Имайте предвид, че обслужващата Ви банка никога няма да изиска да съобщите Вашите пароли.

- След като приключите с Интернет банкирането, винаги проверявайте дали сте излезли от портала и сте отписали профила си.
- Никога не запаметявайте паролата на Вашия компютър, освен ако не е защитена (например: Password manager).
- Никога не оставяйте компютъра си без наблюдение, когато сте влезли във Вашето Интернет банкиране.
- Съветваме ви да променяте периодично Вашата парола. При промяна на паролата, винаги избирайте такава, която трудно може да бъде разгадана.
- Не използвайте паролата си за Интернет банкиране за други уебсайтове.

Погрижете се за сигурността на персоналния си компютър

- Бъдете изключително внимателни към всякакви непоискани имейл съобщения, особено ако са изпратени от непознати адреси. Никога не отваряйте линкове в такива имейл съобщения, подканващи Ви да посетите непознати уеб сайтове.
- Не отваряйте, не изтегляйте или разархивирайте непознати прикачени файлове в имейл съобщения, получени от непознати, подозрителни или несигурни източници.
- Инсталирайте антивирусен софтуер, обновявайте го редовно и периодично сканирайте компютъра си за Ваша сигурност.

Защитете мобилното си устройство

• Защитете Вашия телефон с (нетривиална) парола и задайте автоматично заключване на екрана, когато не се използва. Обмислете поставянето на допълнителна защита - пръстов отпечатък, жестове и други в зависимост от модела и функционалностите на мобилното устройство. По този начин ще увеличите сигурността си при физическа кражба на устройството. Не позволявайте телефонът, от който банкирате, да се използва от други лица без надзор.

• Уверете се, че използвате всички актуализирани средства, препоръчани от Вашия системен доставчик. Чрез тези актуализации производителите отстраняват откритите уязвимости в по-ранните версии на системата.

• Изтегляйте приложения само от официални магазини за приложения (например Apple Store, Google Play Store). В противен случай рискувате да инсталирате в смартфона си зловредни приложения.

• Никога не отключвайте операционната система на вашия смартфон (напр. чрез jailbreak, rooting), тъй като това Ви излага на повече рискове. Root и jailbreak са действия, които позволяват да се използват заключени от производителя функции на телефона и придобиване на администраторски права. Получаването на администраторски права предоставя възможност от злонамерени лица да получат пълен и неоторизиран достъп до цялото Ви устройство.

• Не съхранявайте в смартфона си некриптирани поверителни данни.

• Инсталирайте антивирусен софтуер и редовно го актуализирайте.

Ако имате някакви съмнения относно достоверността на имейл съобщение, което претендира, че е с подател ПроКредит Банк, незабавно ни информирайте на тел. (+359) 2 81 35 100.

Как мога да се защитя от „phishing“?

ПроКредит Банк е ангажирана с предприемане на редица мерки, за да защити Вашите онлайн плащания и да запази целостта на данните във Вашия банков акаунт. За да постигнем това, ние използваме последна версия софтуер за сигурност и прилагаме различни процедури за безопасност. Въпреки това, Ви молим да имате предвид, че Интернет и електронната Ви поща може да бъдат използвани като средство за незаконна дейност. Ето защо, препоръчваме да предприемете няколко прости предпазни мерки, които ще направят онлайн банкирането Ви по-сигурно.

Съвети за избягване на „phishing“

Какво е „phishing”?

„Phishing“ е опит засъбиране на Ваша лична информация чрез изпращане на имейл. Съобщенията обикновено претендират, че са изпратени от истински компании, функциониращи в Интернет пространството, но всъщност целта им е да примамят клиентите на тези компании да разкрият информация на фалшив уеб сайт, използван от измамници.

Каква информация ще поискат от Вас?

„Phishing“ имейлите обикновенно претендират, че е необходимо да обновите или верифицирате Вашия профил и Ви призовават да кликнете на линк от писмото, който Ви отвежда към фалшив уеб сайт. Всяка информация, която е въведена в този уеб сайт се използва от престъпници с цел измама.

Как да избегнем възможността да станем жертва на „phishing“?

Бъдете подозрителни към всички непоискани и неочаквани имейли, които получавате, дори и на пръв поглед да изглеждат от надеждни източници. Електронните писма са изпратени с цел достигане до действителни активни имейл адреси, които принадлежат на клиенти със сметка в институцията - мишени, обект на интерес от страна на измамниците.

Какво трябва да направите, ако получите „phishing“ имейл?

Ако имате съмнения относно достоверността на получено имейл съобщение, което претендира, че е с подател ПроКредит Банк, незабавно ни информирайте като се свържете с нас на тел. (+359) 2 81 35 100 и препратете полученото имейл съобщение на адрес: **probanking@procreditbank.bg**

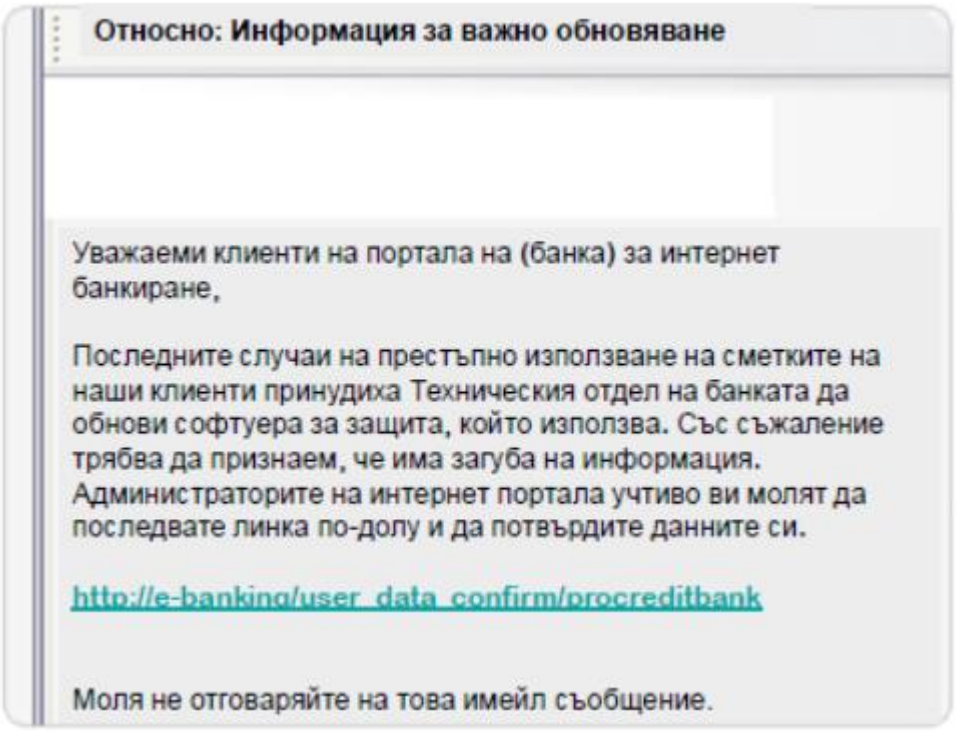
За повече информация посетете следния линк:
http://www.staysafeonline.org/stay-safe-online/keep-a-clean-machine/spam-and-phishing

Допълнителни съвети за онлайн сигурност

Как да разпозная “phishing“ имейл?

„Phishing“ имейла може да изглежда така, че все едно идва от имейл на истинската ПроКредит Банк. За съжаление, поради начина на създаване на имейла, изключително лесно е измамниците да създадат фалшив подател в полето „От: (From)” или да прикрият истинския подател.

Пример за измамно имейл съобщение

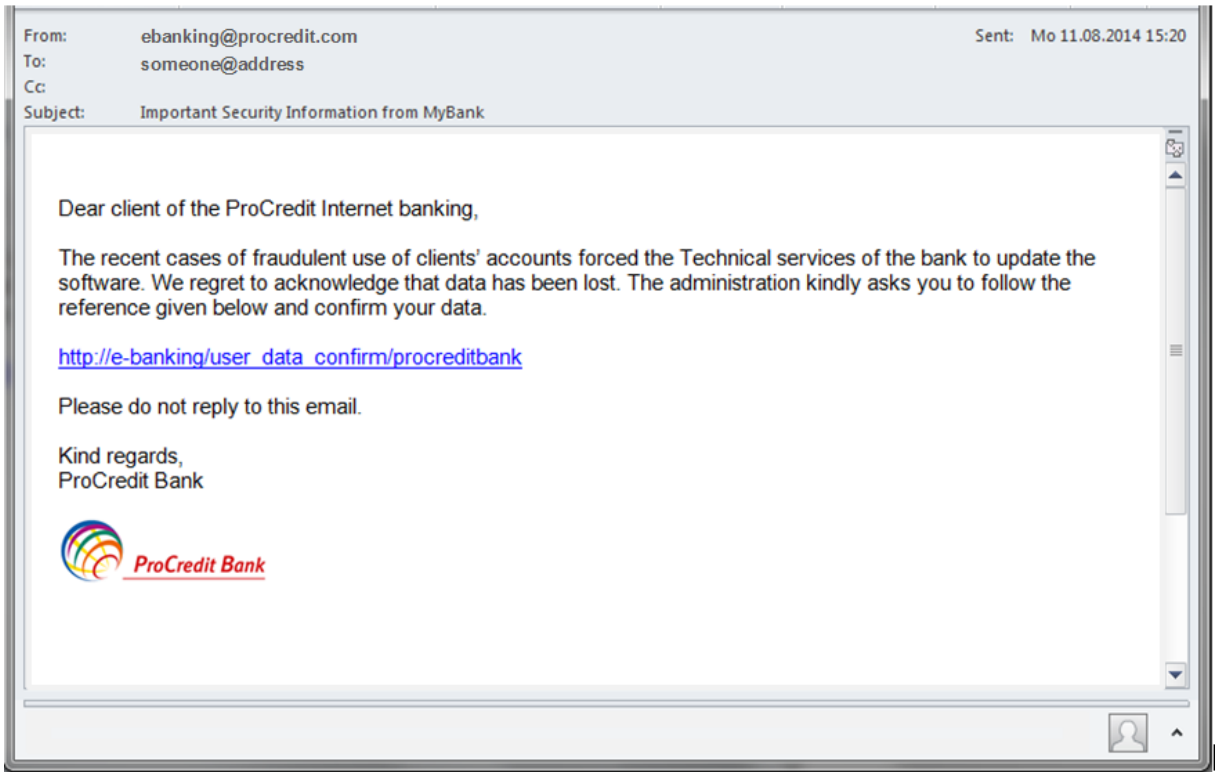

Относно: Информация за важно обновяване

Уважаеми клиенти на портала на (банка) за интернет банкиране,

Последните случаи на престъпно използване на сметките на наши клиенти принудиха Техническия отдел на банката да обнови софтуера за защита, който използва. Със съжаление трябва да признаем, че има загуба на информация. Администраторите на интернет портала учтиво ви молят да последвате линка по-долу и да потвърдите данните си.

http://e-banking/user_data_confirm/procreditbank

Моля не отговаряйте на това имейл съобщение.



Ако имате някакви съмнения относно достоверността на имейл съобщение, което претендира, че е с подател ПроКредит Банк, незабавно ни информирайте на тел (+359) 2 81 35 100 и препратете подозрителните имейл съобщения на адрес: probanking@procreditbank.bg.