СЪВЕТИ ЗА ЗАЩИТА НА ВАШИТЕ ЛИЧНИ ДАННИ

Инвестбанк АД прилага различни защитни механизми, за да защити личните Ви данни и да осигури сигурността на Вашите онлайн плащания при използване на услугата „Интернет банкиране“ и разплащания с банкови карти.

Важно!!!

Инвестбанк АД по никакъв начин няма да поиска от Вас конфиденциална информация, като потребителско име и парола за достъп до Интернет банкиране или информация за банкова карта, като: номер на карта, PIN на карта, дата на валидност или CVV/CVC.

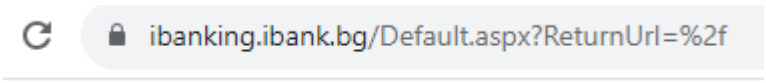
Препоръчваме Ви при най-малко съмнение, че сте станали жертва на измама, да уведомите незабавно Call Center на Инвестбанк АД на телефон 0700 12 555 (за абонати на Виваком на цената на един градски разговор от цялата страна) и да поискате да Ви бъде блокиран потребителският профил за достъп до Интернет банкиране или банковата Ви карта!

Въпреки това, сигурността на Вашата електронна поща и компютърна система могат да бъдат атакувани от различни вируси и зловреден софтуер, с цел кражба на лична информация като: пароли, кодове за достъп до Интернет банкиране, номера на дебитни / кредитни карти, номера на лични документи и др.

Препоръчваме Ви следните мерки, които Вие можете да предприемете, за да се предпазите от евентуална онлайн измама:

- Никога не разкривайте Вашите лични данни по телефона, чрез SMS или мейл;
- Инсталирайте антивирусна програма на компютъра и на мобилното си устройство, извършвайте редовно сканиране с нея и следете за обновяването на нейните дефиниции;
- Използвайте „силни“ пароли;
- Четете внимателно получените от Вас мейли и спазвайте следните препоръки:
  - Ако в мейла има приложена връзка към интернет страница, винаги правете проверка къде ще ви „отведе“ тя, преди да кликнете на нея. Поставете курсора върху URL връзката и проверете дали адресът е същият като този, който се появява във визуализирания прозорец – ако те са различни не отваряйте тази връзка;

  - Не се доверявайте на мейли, които Ви пренасочват към сайтове, на които да попълните вашето потребителско име, парола или друга лична информация;
  - Обърнете внимание на текста. В повечето фалшиви мейли текстът е пълен с правописни и синтактични грешки. Тези грешки създават впечатлението, че текста е писан от някой, който не знае български език. Веднага изтрийте подобен мейл!
- Разпознавайте защитената страница на Интернет банкирането на Инвестбанк АД:
  - Преди да въведете потребителското си име и парола, потърсете доказателство, че уеб страницата, която сте избрали ползва криптиран канал за обмен на данни. Сигурен признак за това, дали получаваните съобщения на екрана си от Интернет банкирането на Инвестбанк АД, е наличието на заключения катинар до адреса.
  - URL лентата изглежда така:



- При проявени съмнения от Ваша страна, относно нетипично или непознато съобщение и/или обстоятелство при ползване на услугата Интернет банкиране на Инвестбанк АД, веднага се обадете в центъра за обслужване на клиенти на телефон **0700 12 555** /за абонати на Виваком на цената на един градски разговор от цялата страна/.

ДОПЪЛНИТЕЛНИ СРЕДСТВА ЗА ЗАЩИТА

Антивирусна защита

Вирусите могат да повредят Вашият компютър, да унищожат данни или, в някои случаи, да изпратят лична информация или пароли, въведени по време на използването на системата, на неоторизирани лица. Ползването на надеждна и актуализирана антивирусна програма ще намали вероятността от подобно нежелано събитие.

Сигурна парола

Използвайте сигурни пароли, които са комбинация от букви, цифри и различни символи като "@", "!" и др. Сменяйте паролата си често - на всеки 1-3 месеца.

Използвайте само проверени компютри

Опитайте максимално да избягвате използването на услугата „Интернет банкиране“ в присъствието на други хора или на публични места (в интернет клубове или на компютри, използвани от други хора, освен Вас). Избягвайте и публични WiFi връзки, незащитени с парола.

Не оставяйте КЕП в компютъра

След приключване на работата с Вашия Квалифициран Електронен Подпис (КЕП), винаги го изключвайте от компютъра и никога не оставяйте устройството/чип-картата без надзор!

Малко повече внимание

Не оставяйте безконтролно личния си мобилен телефон или Тоукън /КЕП/, за да сте сигурни, че не се използват от друг без Ваше знание!

Изход от системата

Важно е след като сте приключили с използването на услугата „Интернет банкиране“, да прекратите сесията, като натиснете бутона „Изход”, а не просто да затворите прозореца на браузъра. Така е сигурно, че защитената връзка, която е била създадена с логването ви в интернет портала, е прекъсната.

ЧЕСТО СРЕЩАНИ ОПИТИ ЗА ИЗМАМА

ФИШИНГ (PHISHING)

Онлайн измама, чиято цел е кражбата на потребителски имена и пароли. Най-често онлайн фишингът започва с мейл, който изглежда, като официално съобщение от надежден източник, например банка или фирма за кредитни карти. Съобщението може да изглежда легитимно и да съдържа запазените знаци на организацията, а мейл адресът да наподобява този на фирмата, от името на която се изпраща съобщението. В мейла получателите се насочват към фалшив уеб сайт, който ги подканва да предоставят конфиденциални данни, като име и парола за достъп до Интернет банкиране, номер на банкова карта, CVV\CVC или други данни свързани с банковата Ви карта, като например кодове за оторизация на

плащане/превод на средства.
НЕ ПРЕДОСТАВЯЙТЕ конфиденциална информация, свързана с достъпа ви до Интернет банкирането или Вашата банкова карта чрез интернет или телефон!

ФАРМИНГ (PHARMING)

Друг метод, използващ фалшиви уеб сайтове, но без e-mail съобщения. Фармингът се осъществява чрез т.н. атака "DNS poisoning" или чрез промяна на "hosts" файла в компютъра на жертвата. По този начин се пренасочва трафика от определен уеб сайт към друг, който е негово копие и има за цел кражбата на секретна информация, като потребителско име, парола и др. При "DNS poisoning" DNS сървърът преобразува адресите на уеб сайтовете, които пишете в адресната лента на уеб браузъра, в IP адреси.
Например, когато напишете www.ibank.bg, компютърът Ви ще се обърне към DNS сървъра на Вашият интернет доставчик, за да научи IP адреса на сайта и да го отвори. Ако той бъде подменен с друг адрес, при изписването на www.ibank.bg, заявката ще бъде пренасочена към сървър, съдържащ точно копие на сайта на Банката.
Потребителят има вероятност да не разбере за измамата, защото е написал правилно и собственоръчно адреса на уебсайта, без да знае, че е жертва на "DNS poisoning" атака.

ВИШИНГ (VISHING)

Вариант на метода фишинг, при който имейлите съдържат телефонен номер. В този случай се препоръчва потребителите да се обадят, за да потвърдят потребителските си идентификатори или друга секретна информация. В имейла може да се крие и вирус, чрез който измамникът заразява компютъра на жертвата и получава пълен достъп до данните, включително до банкови сертификати. Друг вариант на ВИШИНГ е измамно обаждане по телефон, в което измамникът изисква от жертвата споделянето на конфиденциална информация.

В интерес на Вашата сигурност бихме искали да знаете следното:

Опазването на потребителското име и паролата за вход Интернет банкирането е изключителна грижа и отговорност на клиентите.

Phishing съобщенията подканят клиентите да въведат конфиденциални данни (потребителско име, парола, кодове за активиране на m-token, картови данни и т.н.) в сайт-копие на оригиналния. Същото се отнася и за телефони с маскирани номера.

Инвестбанк никога не би искала от Вас предоставяне на кодове за достъп, пароли или детайли на банкови карти по електронна поща или в каквато и да е онлайн форма!

Ние не изпращаме съобщения за деактивирани акаунти, подканящи към попълване на Ваши данни, за да бъде продължен достъпа Ви до услуги на банката. Въвеждайте данните от акаунта си само на легитимната страница на Интернет банкирането ни https://ibanking.ibank.bg

За да повишите многократно сигурността при банкиране от разстояние настоятелно Ви препоръчваме да инсталирате мобилното приложение Ibank mToken, с което ще можете да потвърждавате нареждания по всяко време.

С грижа за Вас,
Екипът на Инвестбанк АД