Курсов проект по „Информационна сигурност“

***Изготвил: Емил Григоров Медаров***

***Специалност: „Информатика“, задочно***

***ФН: 2001262013***

В съвременния дигитален свят, в който информационните технологии проникват в почти всички аспекти на нашия живот, въпросите на информационната сигурност заемат централно място. Всеки ден милиони хора използват онлайн банкиране и други електронни финансови услуги, като подлагат на риск личната си и финансова информация. Този курсов проект по "Информационна сигурност" цели да разгледа важни аспекти на тази тема и да предостави съвети и насоки за подобряване на собствената информационна сигурност.

В хода на този проект ще разгледаме широка гама от техники и методи, които могат да бъдат използвани за подобряване на сигурността на онлайн банкиране и защитата на финансовите данни на потребителите. Ще разгледаме силни пароли, двуфакторна автентикация, измамнически атаки като фишинг и социално инженерство, както и мерки за предотвратяване на тези заплахи.

Също така, ще проучим съвети за сигурно използване на мобилните банкови приложения, включително актуални средства за сигурност и препоръки за поведение при потенциални заплахи. Курсовият проект ще се фокусира и върху физическата и логическата сигурност на устройствата, използвани за банкиране, като подчертава важността на актуализиране на софтуера и защитата на достъпа до тях.

Не на последно място, ще разгледаме какво да правим при съмнение за атака или неоторизиран достъп до банковите ни данни и как да се свържем с официалния контактен център на банката за получаване на помощ и съвети.

Този курсов проект представлява ценен ресурс за всеки, който желае да подобри информационната си сигурност, особено когато става въпрос за финансова информация и онлайн банкиране. Чрез неговата реализация и прилагане на предоставените насоки, потребителите могат да се предпазят от потенциални заплахи и да продължат да използват финансовите си ресурси с повишена сигурност и увереност.

**Съвети за сигурно използване на KBC Online Bulgaria:**

1.Не използвайте обществени компютри за достъп до KBC Online Bulgaria. Ограничете броя на устройствата, които използвате за интернет банкиране и ги оборудвайте с актуализиран антивирусен софтуер.

2.Избягвайте да използвате KBC Online Bulgaria на обществени места или в присъствието на други хора.

3.Ако използвате безжична мрежа (Wi-Fi), уверете се, че тя е защитена със съвременен протокол за сигурна връзка (WPA2 или по-нов). Избягвайте обществени Wi-Fi мрежи, тъй като те могат да бъдат небезопасни.

4.Достъпвайте KBC Online Bulgaria директно чрез адреса https://online.kbcbank.bg без да използвате автоматичното допълване на адресите.

5.Не добавяйте KBC Online Bulgaria като предпочитана връзка в браузъра си, тъй като това може да създаде риск от манипулации от неоторизирани лица.

6.Винаги проверявайте дали уеб страницата, която отваряте, е автентична и сигурна. Уверете се, че връзката е защитена, като проверите за заключен катинар в адресната лента на браузъра си.

7.Използвайте бутона "Изход" на сайта след завършване на банкирането, преди да затворите браузъра.

8.Не запаметявайте потребителските си имена и пароли в браузъра си.

9.Използвайте браузър, който поддържа сигурен протокол за връзка (TLS версия 1.2 или по-нова) и редовно актуализирайте браузъра си.

10.Активирайте автоматичните обновления и филтрите за предотвратяване на фишинг атаки в браузъра си.

11.Не инсталирайте излишни инструментални ленти (toolbars) в браузъра си, освен ако не са абсолютно необходими, за да избегнете риска от зловреден софтуер.

12.При избиране на парола, изберете "силна" парола с дължина от поне осем символа, включваща малки и главни букви, цифри и специални символи. Сменяйте паролата си редовно и не използвайте очевидни пароли.

13.Не споделяйте потребителското си име и парола с други хора и не ги записвайте никъде.

14.Ако трябва да предоставите достъп до сметките си на други лица, изисквайте отделен достъп от банката.

15.Актуализирайте банката си с новия телефонен номер за връзка, когато се наложи. Не посочвайте телефон на близките си.

**Допълнителни средства за сигурност при активно банкиране с KBC Online Bulgaria:**

1.KBC Online Bulgaria предоставя допълнителни средства за сигурност, които потребителите могат да използват, за да потвърдят активни операции. Това включва парола MTAN, която се изпраща чрез SMS съобщение или код, генериран от хардуерно устройство или токен (който може да бъде хардуерно устройство или специализирано приложение за мобилни устройства - софтуерен токен).

2.Парола MTAN чрез SMS съобщение - При удостоверяване на плащания чрез тази парола, получавате SMS съобщение с детайли за транзакцията, включително парола MTAN, сума на транзакцията и последните 10 цифри и букви от IBAN номера на сметката на получателя. Важно е да проверявате тези детайли и да не въвеждате MTAN кода, ако получите SMS без да сте инициирали транзакция или ако има различия в IBAN номера.

3.Хардуерно устройство (токен) - Токен устройството трябва да се съхранява на сигурно място под ваш контрол, и трябва да помните отключващия PIN код, който да не споделяте с никого и да не го записвате на физически носител или на самото устройство.

4.Потвърждение с токен - При удостоверяване на плащания с токен устройство, на дисплея му се изобразяват детайли за транзакцията, включително последните 10 цифри и букви на сметката на получателя, сумата на транзакцията и валутата. Важно е да сравнявате тези детайли и да не потвърждавате транзакцията, ако има разлики в информацията.

5.KBC Online Bulgaria предоставя възможност за използване на групов подпис, където активни операции могат да бъдат потвърждавани от няколко потребителя с различни средства за сигурност, повишавайки така общата сигурност при активните операции. Това е особено полезно за корпоративни цели.

**Операционна система и допълнителен софтуер:**

1.Винаги използвайте актуална операционна система и софтуерни продукти, които поддържат автоматично обновление, ако тази опция е налична. В противен случай, използвайте само официални източници за обновления.

2.Инсталирайте и поддържайте актуален антивирусен софтуер, който да сканира файловете и електронната поща за вируси и други заплахи.

3.Използвайте защитна стена (firewall) на вашия компютър, който банкирате с KBC Online Bulgaria, за да предотвратите нежелани атаки.

4.Внимавайте с софтуера, който инсталирате, и избягвайте използването на програми със съмнителен произход или "кракнат" софтуер, който може да бъде носител на зловреден софтуер.

5.Обръщайте внимание на изтеклите поддръжка на операционната система, като Windows XP, и предприемайте необходимите мерки за поддържане на сигурността.

**Мобилно банкиране чрез специализирани апликации с KBC Mobile Bulgaria:**

1.KBC Mobile Bulgaria предоставя възможност за достъп до интернет банкиране чрез специализирани мобилни приложения за смарт устройства като телефони и таблети, поддържащи операционните системи Android и iOS.

2.За да инсталирате мобилното приложение на KBC Mobile Bulgaria, използвайте официалните маркети - Google Play Store за Android, AppGallery за Huawei и App Store за iOS. Този метод на инсталиране осигурява, че приложението е официално и безопасно.

3.За достъп до мобилното приложение, използвайте същите потребителско име и парола, както и за стандартното интернет банкиране. Освен това, мобилното приложение предлага възможност за конфигуриране на ПИН и/или биометрични данни (когато са поддържани от устройството) за по-удобен и бърз достъп.

4.За активиране на опцията за вписване с биометричен отпечатък, потребителят трябва да направи съответните настройки на своето устройство. Важно е да се отбележи, че при iOS операционни системи, всеки, който има достъп до биометричния отпечатък на устройството, ще има достъп и до профила за KBC Mobile Bulgaria, който използва биометрия за вписване. Отбелязваме, че биометричните данни не се съхраняват и не се обработват от ОББ АД.

5.Мобилното приложение поддържа известия в реално време (push notifications), които могат да бъдат активирани от настройките на профила. Важно е да се отбележи, че известията се изпращат на последното устройство, от което потребителят се е вписал в своя профил в KBC Mobile Bulgaria.

6.Допълнителни средства за сигурност, които могат да се използват при активно банкиране чрез мобилните апликации, включват MTAN парола чрез SMS и хардуерно устройство (token). При използването на MTAN парола чрез SMS, е препоръчително да настроите получаването на оторизационния код на друг телефонен номер, различен от този, който е свързан с мобилното устройство.

7.За повишаване на сигурността на своето смарт устройство, можете да добавите допълнителни защитни мерки като парола за отключване, разпознаване на лице или пръстов отпечатък, в зависимост от възможностите на устройството. Не споделяйте своето устройство с други лица без надзор.

8.Инсталирайте антивирусен софтуер от надеждни производители и го актуализирайте редовно. Важно е да използвате официални маркети за инсталирането на антивирусния софтуер.

9.Винаги актуализирайте операционната система на своето смарт устройство до последната версия, като използвате инструкциите на производителя.

10.Не използвайте руутнати (root) или jailbreak устройства за банкиране, тъй като те могат да представляват риск за сигурността на вашите данни и финансовата информация.

Обезпечаването на сигурността на вашите мобилни устройства е от съществено значение при използването на мобилните банкиране приложения, и трябва да се спазват съответните мерки за защита.

**Фишингът, социалното инженерство и начините на комуникация:**

**Фишингът (phishing)** е хитрост, с която злоумишленници се опитват да измамят потребителите на компютри и други устройства, свързани с интернет, с цел получаване на техните лични или финансови данни. Те често изпращат измамни имейли или водят потребителите към фалшиви уеб сайтове, където им се иска да предоставят чувствителна информация, като потребителски имена и пароли за достъп до ***KBC Online Bulgaria***. Тези фалшиви уеб сайтове изглеждат много подобно на официалния сайт, но на практика са **измамни**. Отбелязваме, че ОББ АД **никога** не изпраща имейли с линкове, които Ви насочват към страници, на които да въвеждате Вашия потребител и парола. Затова винаги въвеждайте адреса на KBC Online Bulgaria ръчно в уеб браузъра си, за да се осигурите, че влизате в истинския сайт, без да разкривате данните си на трети лица.

Някои интернет браузъри са оборудвани с вградени механизми за предотвратяване на **фишинг атаки**, докато други предоставят възможност за добавяне на допълнения (add-ons), които предоставят допълнителна защита срещу този вид атаки.

**Социалното инженерство** представлява опит от страна на злоумишленници да заблудят потребителите, като се представят като служители на банката, които се опитват да получат поверителна информация в телефонни разговори, чатове или имейли. Те могат да представят сценарии, при които се налага да разкриете лични данни или да инсталирате софтуер на Вашето устройство. Отбелязваме, че ОББ АД никога не изпраща електронни съобщения или чат съобщения, в които Ви моли да споделите пароли, потребителски имена, банкови сметки и други чувствителни данни. Служителите на ОББ АД няма да Ви помолят за такава информация по телефона.

ОББ АД също така не изпраща съобщения, които Ви насочват да се свържете на посочения телефонен номер в съобщението, за да предоставите информация, свързана с Вашия акаунт в KBC Online Bulgaria.

Също така, ОББ АД няма да Ви насочи към инсталиране на софтуер за отдалечен контрол, като Team Viewer, AnyDesk, VNC и други, с цел дистанционен достъп и контрол над Вашето устройство.

Ако имате съмнения относно истинността на определено съобщение, което сте получили чрез чат, имейл или телефонно обаждане, не се колебайте да се свържете с ОББ АД на официалния им телефонен номер или имейл адрес, за да потвърдите легитимността на съобщението.

За да поддържате сигурността на Вашите финансови данни и лична информация, винаги бъдете внимателни и предпазливи при обработката на всякакви искания за предоставяне на чувствителна информация, дори ако изглеждат легитимни.

***Мерки, които могат да се предприемат за повишаване на нивото на информационната сигурност на системата за онлайн банкиране:***

**1.Силни пароли и двуфакторна автентикация (2FA):**

* Използвайте силни пароли, които да съдържат комбинация от букви (главни и малки), цифри и специални символи.
* Активирайте двуфакторната автентикация (ако вашият банк предлага такава услуга). Тя ще увеличи сигурността, тъй като изисква втора стъпка за потвърждение на вашата самоличност.

**2.Софтуер и операционна система:**

* Редовно актуализирайте операционната система на вашия компютър или мобилно устройство.
* Инсталирайте актуални антивирусни програми и персонални защитни стени на устройствата, от които банкирате.

**3.Използвайте официални приложения и уебсайтове:**

* За достъп до банковите услуги използвайте само официалните мобилни приложения и уебсайтове на банката. Не се доверявайте на непознати линкове или приложения.

**4.Бдителност при получаване на съобщения:**

* Внимавайте с имейл съобщения и текстови съобщения (SMS), които се опитват да ви подканят да предоставите лична информация или да извършите финансови транзакции. Винаги проверявайте изпращача и линковете, преди да кликнете на тях.

**5.Сигурно мобилно банкиране:**

* За мобилното банкиране използвайте само официални приложения, предоставени от банката.
* Активирайте биометрични методи за вход, ако устройството ви ги поддържа.
* Разгледайте възможността за използване на допълнителни средства за сигурност като MTAN парола и хардуерни токени.

**6.Обучение и осведоменост:**

* Научете се за различните видове атаки като фишинг и социално инженерство, за да бъдете по-бдителни и да разпознавате потенциални опити за измама.

**7.Свържете се с Контактния център:**

* Ако имате дори и най-малки съмнения или въпроси, не се колебайте да се свържете с Контактния център на банката чрез посочените телефони и имейл адрес. Те ще ви предоставят помощ и информация.

**8.Редовно преглеждайте банковите извлечения:**

* Проверявайте редовно вашите банкови извлечения и транзакции, за да забележите неправомерни или непознати транзакции и да реагирате навреме.

**9.Избягвайте използването на обществени Wi-Fi мрежи:**

* Избягвайте да извършвате банкови операции чрез обществени Wi-Fi мрежи, тъй като те могат да бъдат незащитени и податъците ви да бъдат компрометирани.

**10.Защита на физическата сигурност на устройствата си:**

* Пазете устройствата си под контрол и ги заключвайте с пароли, PIN-кодове, пръстови отпечатъци и други методи за физическа защита.