

## *Киберпреступления*

### *Вишинг*



**Вишинг** – один из методов мошенничества с использованием социальной инженерии. Злоумышленник, используя телефонную связь и играя определённую роль (сотрудника банка, покупателя и т.д.), под разными предложениями пытается выманить у держателя банковской платежной карты (далее – БПК) конфиденциальную информацию, или побуждает к совершению определенных действий со своим банковским счетом или платежной картой.

## ВНИМАНИЕ! ОПЕРАЦИЯ «ВИШИНГ»!

АФЕРИСТ МОЖЕТ  
ПОВОНИТЬ ПО ПОВОДУ  
ТОВАРА НА ТОРГОВОЙ  
ПЛОЩАДКЕ И  
ПРЕДЛОЖИТЬ СДЕЛКУ С  
ПРЕДОПЛАТОЙ



АФЕРИСТ МОЖЕТ  
ПРЕДСТАВИТЬСЯ  
БАНКОВСКИМ РАБОТНИКОМ И  
ВЫМАНИТЬ  
КОНФИДЕНЦИАЛЬНЫЕ  
ДААННЫЕ



АФЕРИСТ СООБЩАЕТ,  
ЧТО РОДСТВЕННИК  
ЖЕРТВЫ ПОПАЛ В БЕДУ  
И ЕМУ НУЖНА  
ФИНАНСОВАЯ ПОМОЩЬ



**ВИШИНГ** - СПОСОБ МОШЕННИЧЕСТВА С ПОМОЩЬЮ ТЕЛЕФОНА, КОГДА МОШЕННИК ПОД РАЗЛИЧНЫМ ПРЕДЛОГОМ ПЫТАЕТСЯ ВЫМАНИТЬ ПЕРСОНАЛЬНУЮ ИНФОРМАЦИЮ ЖЕРТВЫ ДЛЯ ПОСЛЕДУЮЩЕГО ХИЩЕНИЯ ДЕНЕГ С ЕЕ БАНКОВСКОГО СЧЕТА

- НИКОГДА НЕ СООБЩАЙТЕ  
НЕЗНАКОМОМУ СВОИ  
ПЕРСОНАЛЬНЫЕ ДАННЫЕ

- НЕ ТОРОПИТЕСЬ ВЫПОЛНЯТЬ  
ТО, ЧТО ОТ ВАС ПРОСИТ  
СОБЕСЕДНИК. МОШЕННИКИ  
ОЧЕНЬ ИЗОБРЕТАТЕЛЬНЫ И  
УБЕДИТЕЛЬНЫ!



- НАДЕЖНО ЗАЩИЩАЙТЕ СВОИ  
ДААННЫЕ (ДВУХФАКТОРНАЯ  
АВТОРИЗАЦИЯ,  
СМС-ОПОВЕЩЕНИЕ, И Т.Д.)

- В СЛУЧАЕ УТЕРИ ИЛИ КРАЖИ  
КАРТЫ ЗАБЛОКИРУЙТЕ ЕЕ ПО  
ТЕЛЕФОНУ ИЛИ В БАНКЕ

## Как распознать вишинг?

В последнее время наибольшее количество звонков поступает потенциальным жертвам якобы от представителей банков. Как правило, по мобильному телефону преступник под видом уточнения информации о переводе крупной суммы денег выведывает у жертвы реквизиты доступа к банковскому счету и выводит оттуда все деньги. При этом расчет делается на быстроту, шоковое состояние озадаченной жертвы, коммуникативную убедительность преступника.

# ВНИМАНИЕ! УЧАСТИЛИСЬ СЛУЧАИ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА!

**МОШЕННИК** МОЖЕТ ПРЕДСТАВИТЬСЯ:      И НАЗВАТЬ **ПРИЧИНУ** ЗВОНКА:



- сотрудником Банка;
  - сотрудником службы безопасности Банка;
  - сотрудником финмониторинга;
  - сотрудником больницы;
  - сотрудником благотворительной организации;
  - родственником.
- ваша карта заблокирована;
  - в отношении вашей карты предпринимаются мошеннические действия;
  - вашему родственнику нужна помощь или лечение;
  - вам положена отсрочка по кредиту или пособие.

ОН МОЖЕТ **ПОПРОСИТЬ**:

Данные карты:



- номер карты;
- CVV/CVC-код;
- PIN-код;
- срок действия карты.

Пароль:



- от интернет-банка;
- из SMS-сообщения  
(для входа в интернет-банк или подтверждения операции).

Перевести деньги:



- на специальный счет или карту, где они будут в безопасности.

# НЕ

- сообщайте никому данные карты;
- сообщайте никому пароли и коды из SMS;
- выполняйте действия с банковской картой по просьбе третьих лиц.

Зачастую такие преступления осуществляются с подменой входящего телефонного номера. При входящем звонке жертва видит на экране мобильного телефона либо подменный номер, либо даже короткий номер банка: современные протоколы мобильной телефонии и различный софт позволяют осуществлять телефонные звонки анонимно. Свои услуги в этом предлагают различные платные сервисы и сайты. Самым популярным сервисом для подмены телефонного номера является «Changing number», который взимает плату за предоставление своих услуг, а также за каждую минуту звонка, в соответствии с выбранным тарифным планом.

## КАК ПОНЯТЬ, ЧТО С ВАМИ ГОВОРIT МОШЕННИК

**Собеседник представляется сотрудником банка и:**

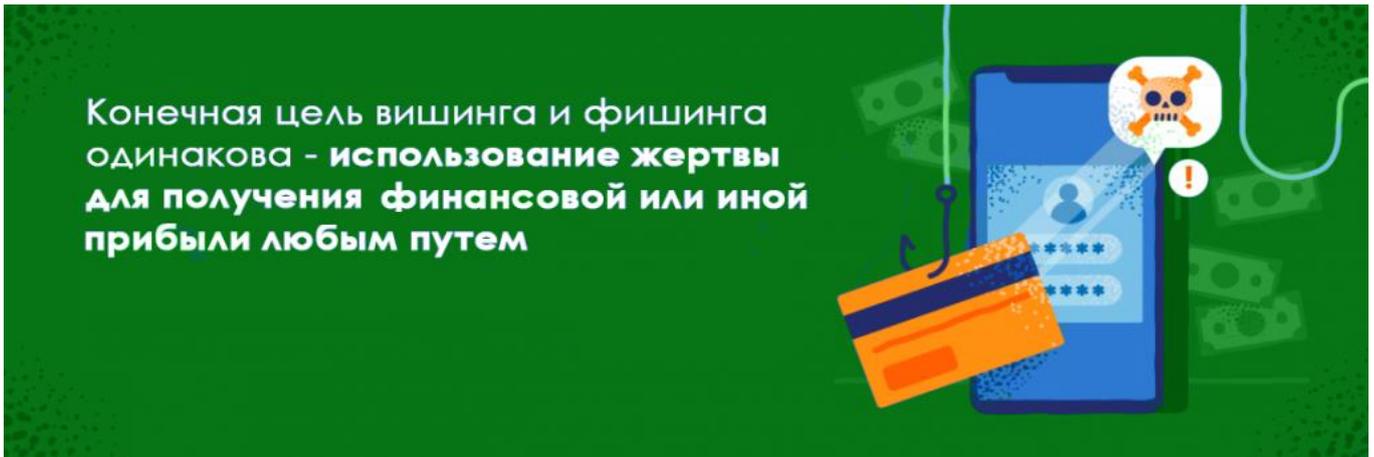


- сообщает о **блокировке** вашей карты
- говорит, что аферисты хотят **похитить** деньги со счета или оформить от вашего имени **кредит**
- просит назвать **реквизиты** карты, **срок** ее действия, **свс/cvv-** и **sms-коды**
- рекомендует экстренно перевести все деньги на «**безопасный**» счет
- убеждает **перейти по ссылке** для отмены операции
- отправляет вас в банк оформить «**зеркальный**» кредит и перечислить деньги на **резервный счет**
- заверяет, что необходимо установить специальное **приложение для безопасности**

**ЕСЛИ СОБЕСЕДНИК ПРЕДЛАГАЕТ ВЫПОЛНИТЬ ЧТО-ТО ИЗ ПЕРЕЧИСЛЕННОГО:**

- **НЕ СОВЕРШАЙТЕ** НИКАКИЕ ОПЕРАЦИИ ПО СЧЕТАМ
- **ПРЕРВИТЕ** РАЗГОВОР
- **ЗАБЛОКИРУЙТЕ** АБОНЕНТА
- ПОЗВОНИТЕ НА **ГОРЯЧУЮ ЛИНИЮ** ВАШЕГО БАНКА ПО НОМЕРУ С ОБРАТНОЙ СТОРОНЫ КАРТЫ

Вторым по актуальности киберпреступлением, совершаемым с использованием методики вишинга, является обман клиентов торговых онлайн-площадок. Продавцу, разместившему на такой торговой площадке объявление о продаже товара, поступает звонок или сообщение от незнакомца (либо сообщение в соцсетях или мессенджерах), который якобы заинтересовался вещью и готов перевести предоплату на счет продавца. Обманутый продавец сообщает конфиденциальную информацию мошеннику, и тому остается только получить доступ к счету и снять деньги.



В последнее время учатившимися случаями вишинга становится «звонки из банка». **Звонящий представляется сотрудником службы безопасности банка** и уверяет: «С вашей карты кто-то хотел похитить деньги, для отмены операции назовите свои данные». Выманив сведения, мошенник выводит со счета все средства и исчезает.



## Как не попасться?

Скажите, что вы не клиент этого учреждения (даже если это так). Если на той стороне мгновенно переключат на «специалиста из вашего банка» – это точно мошенничество. Или просто положите трубку и перезвоните в банк сами. Только номер телефона смотрите не во «Входящих звонках», а на сайте банка.

## Как не стать жертвой киберпреступника.

# ЗАЩИТА БАНКОВСКОЙ КАРТЫ

### Наиболее распространенные методы работы злоумышленников



выманивание реквизитов банковских платежных карт с использованием взломанных аккаунтов знакомых в социальных сетях



**ЛЖЕПОКУПАТЕЛЬ** - под видом покупателя злоумышленник связывается с продавцом, предлагает внести залог перед покупкой товара, а для получения денежного перевода предоставляет ему ссылку на мошеннический сайт, визуально похожий на официальный сайт банка



**ВИШИНГ** - представляясь по телефону сотрудником банка, злоумышленник пытается узнать у держателя карты конфиденциальную информацию (ее реквизиты, а также номер паспорта, личный идентификационный номер, логины, пароли, СМС-коды)



### НЕ СООБЩАЙТЕ НИКОМУ

- информацию, размещенную на вашей банковской платежной карте (на обеих сторонах): номер, дату, код
- цифровые или буквенные коды
- паспортные данные



### ЕСЛИ ВАМ ПОСТУПИЛ СОМНИТЕЛЬНЫЙ ЗВОНОК

- немедленно завершите разговор
- обратитесь в контакт-центр банка, выпустившего карту
- следуйте рекомендациям сотрудника банка



Для защиты денежных средств клиентов у банка есть вся необходимая информация



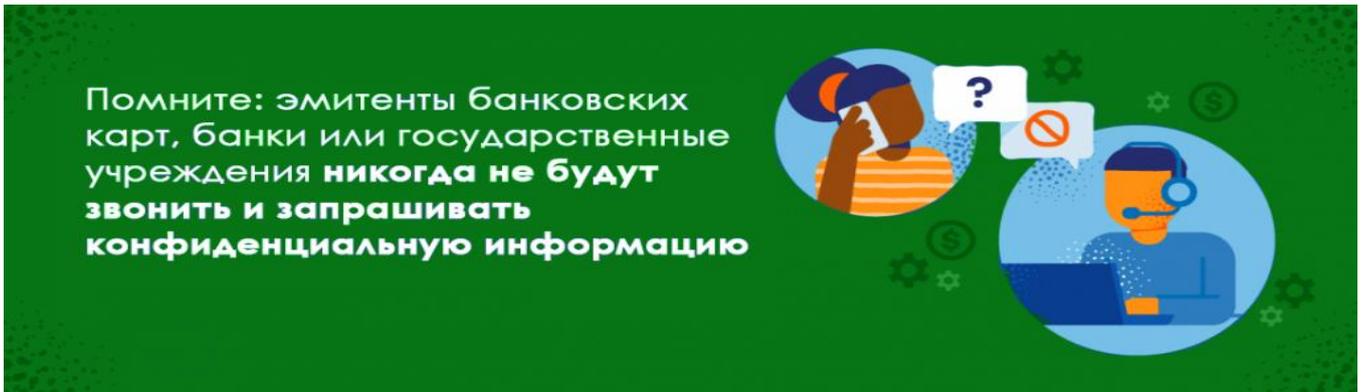
Работники банка по телефону не должны спрашивать ни реквизиты карты, ни паспортные данные



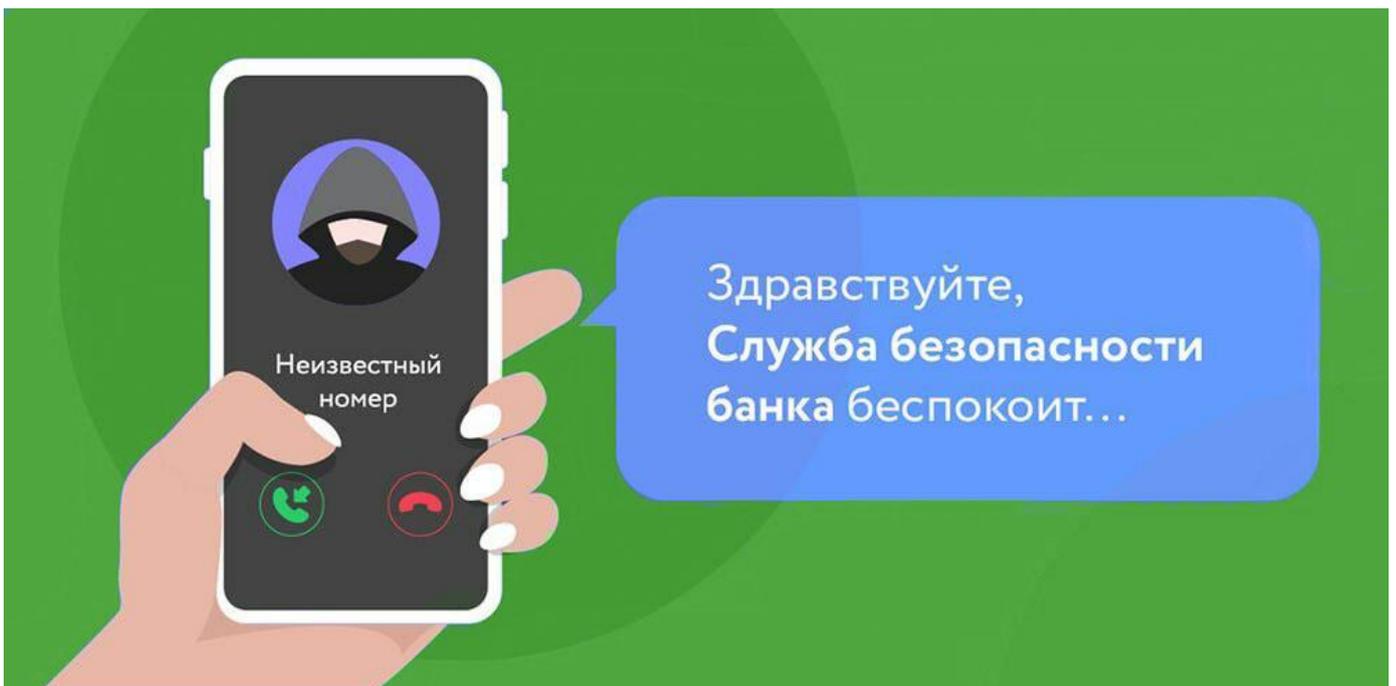
Не давайте никому свой мобильный телефон и предупредите об этом ваших близких, особенно детей и лиц пожилого возраста

## Правила безопасности

В любом случае, чтобы не потерять денежные средства и не раскрывать данные о своей БПК, не следует отвечать на явно подозрительные звонки и SMS, тем более с незнакомых номеров.



Сотрудникам банков, также, как и других организаций, не требуется знать реквизиты вашей БПК для осуществления своей деятельности. Поэтому у вас не может возникнуть обстоятельств, при которых необходимо их сообщать посторонним лицам, кем бы они ни представлялись. В случае получения тревожных сообщений и звонков из банков и иных финансовых или почтовых учреждений, вместо того чтобы идти на поводу неизвестных, следует обязательно самостоятельно перезвонить в учреждение, сотрудником которого представился неизвестный, и уточнить все детали.



**Самые базовые действия, которые должен знать каждый пользователь БПК:**

Важно  
знать

- Не раскрывайте данные, которые у вас просят (данные БПК, логины, пароли, коды из sms);
- Прервите разговор и сами перезвоните в банк, по номеру на сайте банка;
- Не поддавайтесь панике и не позволяйте манипулировать вами;
- Не выполняйте действия с БПК по указанию посторонних, кем бы они не представлялись.

## МОШЕННИКИ «НА КАРАНТИНЕ»: ВИШИНГ

**ЛУЧШЕ НЕВЕЖЛИВО ПРЕРВАТЬ РАЗГОВОР, ЧЕМ ВЕЖЛИВО СООБЩИТЬ PIN-КОД КАРТЫ.**

Сотрудники банка никогда не попросят у вас данные по карте. А чтобы убедиться, что звонок был от мошенников, нужно звонить на официальный номер вашего банка.



**НЕ СПЕШИТЕ РАСКРЫВАТЬ ПЕРВОМУ ЗВОНЯЩЕМУ СВОИ ДАННЫЕ, В БАНКЕ ИХ ИТАК ЗНАЮТ.**

Банки никогда не звонят сами, чтобы спросить по телефону: полный номер карточки; срок ее действия; CVC/CVV; логин и пароль к интернет-банкингу; кодовое слово, код из SMS-сообщения.



**НЕ ПОДДАВАЙТЕСЬ ПАНИКЕ, ЕСЛИ ВАС ПОПЫТАЮТСЯ НАПУГАТЬ ТЕЛЕФОННЫЕ МОШЕННИКИ.**

На паническое заявление о том, что с вашей картой серьезная проблема лучший ответ: «Сейчас позвоню или схожу в банк, чтобы проверить это лично». Будьте уверены – звонящий тут же отключится. Это очень распространенная уловка – напугать владельца карты.



**ОАО «Евразийский Сберегательный Банк», информирует:**

Внимательность следует проявлять также потому, что основная опасность такого мошенничества состоит в том, что в банковских учреждениях отказывают клиентам в возврате денежных средств по операциям, осуществленным не санкционированным держателем БПК и совершенными с использованием технологии аутентификации держателя БПК посредством системы дистанционного банковского обслуживания. Другими словами, в случаях, когда жертва сама сообщает злоумышленникам реквизиты своей БПК, в результате чего совершается хищение денежных средств, результат подобных операций практически невозможно оспорить.

Важно  
знать

**Банки никогда не спрашивают коды и пароли, а также данные БПК, которые они выдали клиентам:**

- **ни по телефону (также sms)**
- **ни в мессенджерах**
- **ни по электронной почте!**

ОАО «Евразийский Сберегательный Банк» убедительно просит вас, ни в коем случае не поддаваться на подобного рода манипуляции, оберегать данные вашей БПК и не разглашать их, как бы убедительно не звучали аферисты на линии.

Уважаемые клиенты, если же реквизиты Вашей БПК были скомпрометированы или вы имеете на это подозрения или в случае утери БПК, позвоните в Банк или примите иные меры к скорейшей ее блокировке. С заблокированного счета Вам без каких-либо затруднений и комиссий выдадут все денежные средства по предъявлению паспорта.

**Заблокировать БПК** можно с помощью мобильного приложения или сообщив в Банк (тел.:+996 312 38 91 91 доб. 167) либо в ЗАО «Межбанковский процессинговый центр» любым доступным способом (в письменной, электронной, очной, устной формах, по указанным номерам) для своевременного блокирования доступа к денежным средствам. Чаще проверяйте информацию о балансе на ваших счетах в мобильном приложении или личном кабинете интернет-банкинга.

**Контактный номер ОАО «Евразийский Сберегательный Банк»: +996 312 38 91 91 (167)**

**Контактный e-mail ОАО «Евразийский Сберегательный Банк»: office@esb.kg**

**Контактный номер ЗАО «Межбанковский процессинговый центр»: +996 312 63 76 96**

Банк не несет ответственности за утерю клиентом конфиденциальной информации, передачу личных данных при использовании непроверенных интернет-ресурсов, а также за транзакции, осуществленные мошенниками на мошеннических сайтах.

**Делитесь этой информацией с близкими, особенно с пожилыми людьми и детьми, снизив тем самым риск мошенничества по Вашей БПК, чтобы мошенники не смогли обмануть Вас!**