

# Как не стать жертвой киберпреступлений

Достижения науки и техники, создание всемирной сети интернет позволили преступности выйти на новый уровень и захватить киберпространство.

Теперь преступнику не нужен прямой контакт с жертвой, он может стать угрозой для каждого пользователя «глобальной паутины», крупных корпораций и целых государств.

Преступность в виртуальном пространстве – явление относительно новое, но часть преступлений, совершаемых в сфере высоких технологий, – это знакомые кражи, мошенничества, вымогательство.

Киберпреступность – незаконные действия, которые осуществляются людьми, использующими информационные технологии для преступных целей. Среди основных видов киберпреступности выделяют распространение вредоносных программ, взлом паролей, кражу номеров кредитных карт и других банковских реквизитов, а также распространение противоправной информации с использованием сети Интернет.

Правила, которые помогут Вам не стать жертвой киберпреступлений:

– храните номер карточки и ПИН–коды в тайне;

– не используйте один пароль для всех интернет-ресурсов;

– к своей основной карте в Вашем банке выпустите дополнительную, которой будете расплачиваться в интернете. Туда легко можно будет переводить небольшие суммы денег, и в случае компрометации данных достаточно просто заблокировать ее;

– регулярно проверяйте состояние своих банковских счетов, чтобы убедиться в отсутствии «лишних» и странных операций;

– поставьте лимит на сумму списаний или перевода в личном кабинете банка;

– не перечисляйте деньги на электронные кошельки и счета мобильных телефонов при оплате покупок, если Вы не убедились в благонадежности лица/организации, которым предназначаются Ваши средства;

– не переводите денежные средства на счета незнакомых лиц;

– не перезванивайте и не направляйте ответные SMS, если Вам поступило сообщение о блокировании банковской карты. Свяжитесь с банком, обслуживающим Вашу карту;

– будьте осмотрительны в отношении писем с вложенными картинками, поскольку файлы могут содержать вирусы. Открывайте вложения только от известных Вам отправителей и всегда проверяйте вложения на наличие вирусов, если это возможно;

– не переходите необдуманно по ссылкам, содержащимся в спам-рассылках. Удостоверьтесь в правильности ссылки, прежде чем переходить по ней из электронного письма;

– не заполняйте полученные по электронной почте формы и анкеты. Личные данные безопасно вводить только на защищенных сайтах;

– насторожитесь, если от Вас требуют немедленных действий или представляется чрезвычайная ситуация. Это тоже может быть мошенничеством, преступники вызывают у Вас ощущение тревоги, чтобы заставить Вас действовать быстро и неосмотрительно;

– не размещайте в открытом доступе и не передавайте информацию личного характера.



## Рассмотрим самые распространенные схемы мошенничества:

### 1. «Звонок из Банка»

Вам звонит незнакомец. Номер входящего звонка очень похож на номер банка, а звонящий представляется работником контакт-центра или службы безопасности банка.

Для реализации мошеннической схемы также используются мессенджеры, прежде всего Viber. Входящий звонок максимально закамуфлирован под звонок сотрудника банка: на аватарке может использоваться логотип банка (полностью или частично), а отображаемый телефонный номер звонящего может быть очень похож на телефон службы поддержки банка.

У мошенников есть возможность звонить с номеров, похожих на официальные номера банка. Злоумышленники меняют цифры в номере, которые вы можете не заметить.

#### У вас просят конфиденциальные данные

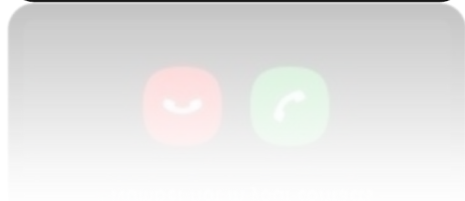
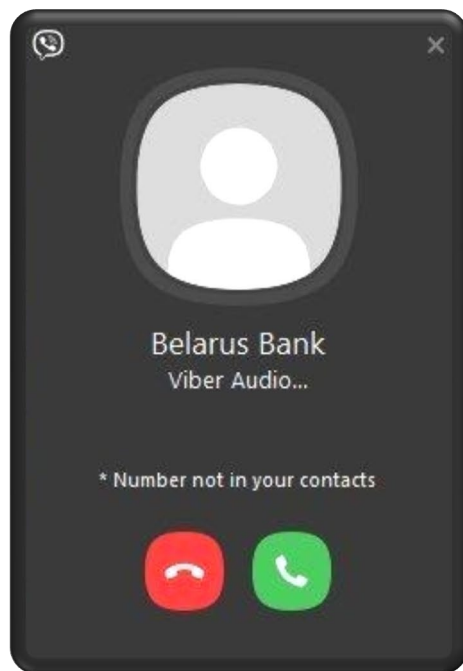
Мошенник сообщает, что «банк выявил подозрительную операцию по Вашей карте» или «поступил запрос на онлайн-оформление кредита на Ваше имя».

Он просит у вас логин и пароль от Интернет-банкинга, код из SMS от Банка (в большинстве случаев сопровождаемый фразой «Никому не сообщайте!»), реквизиты карты (полный номер карты и срок ее действия, CVV- или CVC-код). Это нужно якобы «для сохранности ваших денег».

#### Как мошенник пытается вас убедить

- *«Мы звоним с официального номера, проверьте на сайте».*
- *«В целях конфиденциальности я включаю робота, который защитит ваши данные»* (вы слышите в трубке лёгкий шелест).
- Для убедительности он называет ваши персональные данные (имя, отчество, последние 4 цифры карты и др.) и просит перевести деньги *«на защищённый счет, который закреплён за персональным менеджером: это нужно для безопасности, а потом вы сможете вернуть деньги».*
- Или просит назвать ваши персональные данные или секретные коды из SMS роботу, при этом в трубке вы слышите музыку.
- Вам предлагают услуги страховки от мошеннических действий. Для ее оформления необходимо предоставить данные о карте, на которой находятся значительные денежные средства и SMS-код для подтверждения операции.

**Важно!** Никому не сообщайте свои личные данные, данные карт, защитные коды, коды из SMS! Если с картой, действительно, происходят мошеннические операции, Банк сам может ее заблокировать!



## 2. «Потенциальный покупатель»



Мошенник представляется потенциальным покупателем товара, объявление о продаже которого было размещено вами в сети интернет. По каким-то причинам «покупатель» не может сегодня привезти деньги, но хочет прислать вам залог из другого города по системе дистанционного банковского обслуживания.

### Ссылка

Для проверки поступления перевода мошенник направляет вам ссылку на фишинговый сайт, который очень близок по дизайну на используемый вами интернет-банк или страницу для ввода реквизитов карточки для получения уже отправленного перевода денежных средств. После введения вами в поля фишингового сайта пароля и логина или реквизитов вашей карточки, данные становятся доступны мошеннику.

### QR-код

Вместо ссылки мошенник может направить вам QR-код, который также хранит в себе ссылку на фишинговый сайт. После введения вами в поля фишингового сайта пароля и логина или реквизитов вашей карточки, данные становятся доступны мошеннику.

**Важно!** Не переходите по подозрительным ссылкам. Для веб-версии Интернет-банкинга используйте только официальный сайт Банка, а для мобильной версии – только мобильное приложение, загруженное из официальных магазинов. Внимательно изучите сайт, на котором вводите личные данные. Обязательно проверьте наличие такого сайта в интернете.

**Запомните!** Для получения перевода денежных средств нет необходимости вводить срок действия карты и CVV-код.

## 3. «Сообщения в социальных сетях»

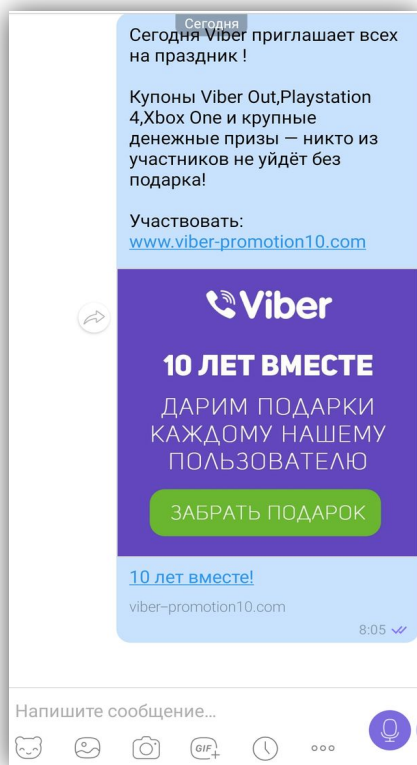
Мошенник незаконным путем получает доступ к страничке в социальной сети и отправляет сообщения с просьбой финансовой помощи от имени ее владельца друзьям.

Просьба может быть самая разная: от «Скинь мне денег на карту, по дружбе» до нехватки денег на большую покупку. В редких случаях мошенник даже просит произвести оплату самостоятельно, обещая возместить затраты при личной встрече.



**Важно!** При получении сомнительного сообщения или малейшей неуверенности в том, что вы действительно общаетесь с владельцем странички, позвоните ему.

#### 4. «Розыгрыши/раздачи/опросы от Банка или иных организаций»



Мошенники оставляют выдуманную рекламу в популярных социальных сетях об опросе от имени Банка и «Раздаче призов первой 1000 прошедших опрос!» или о том, что в связи с годовщиной Банка либо иным значимым мероприятием, последний раздает своим клиентам денежные призы. Цель опроса — якобы изучить мнение клиентов. После прохождения опроса организатор обещает денежное вознаграждение.

Однако, после прохождения опроса необходимо заплатить небольшую комиссию, связанную с перечислением вознаграждения либо с целью получения последнего — ввести данные Вашей банковской карты.

Данный кейс очень разнообразен и ограничивается только воображением мошенников. Вместо опроса может предлагаться возмещение налоговых выплат, компенсация за наличие ваших данных в базе «утечки» и иные махинации.

**Важно!** Посетите официальную страницу организации или позвоните в контакт-центр для проверки наличия акции, розыгрыша или опроса.