**Сопроводительный текст к слайдам**

**Слайд 1**

Существуют общие правила поведения с кибермошенниками. Следуя им, вы сможете себя обезопасить:

− не сообщайте никому личные (данные паспорта, ИНН, дату рождения, адрес места жительства и другие) и финансовые (номер, срок действия, трехзначный код с оборотной стороны карты) данные. Переданные мошенникам личные и финансовые данные могут быть использованы как для самого хищения, так и для оформления кредитов, передачи третьим лицам и для других противоправных действий;

− установите антивирусные программы на все свои гаджеты. Данное ПО предупредит вас в случае установки подозрительного продукта на ваш гаджет. Важно регулярно обновлять антивирусную базу.

− не читайте сообщения и письма от неизвестных адресатов и не перезванивайте по неизвестным номерам. Подобные письма могут содержать в себе вредоносное ПО или фишинговую ссылку, а звонки на неизвестные пропущенные телефонные номера могут быть чреваты как минимум списанием значительной суммы с вашего мобильного счета, а как максимум − быть поводом для мошенников активизировать против вас мошенническую схему;

− не переходите по сомнительным ссылкам и не скачивайте неизвестные файлы или программы. Сомнительные ссылки могут быть опасны для вашего гаджета наличием вируса или вредоносного ПО на сайте, на который они ведут, а скачивание программ с неофициальных источников может дать мошенникам доступ к вашему гаджету;

− заведите отдельную банковскую карту для покупок в Интернете. Перед покупкой переводите на нее ровно ту сумму, которая нужна. Даже если мошенники получат доступ к этой карте, они не смогут похитить больше тех средств, которые были на ней.

**Слайд 2**

В случае если вам позвонили и представились якобы сотрудником банка, положите трубку и самостоятельно позвоните в свой банк по номеру телефона, указанному на обратной стороне карты или на официальном сайте банка. Не нужно перезванивать на номера, с которых вам звонили, – вы рискуете попасть на мошенников. Чтобы связаться с банком, самостоятельно наберите номер, указанный на обратной стороне вашей банковской карты или на официальном сайте кредитной организации.

Для того чтобы обезопасить свои данные, установите двухфакторный способ аутентификации (например, логин и пароль, а также подтверждающий код из СМС) – это, как правило, бесплатно. Пользуйтесь только проверенными и официальными сайтами финансовых организаций в поисковых системах (Яндекс, Mail.ru), помеченными цветным кружком с галочкой.

**Слайд 3**

Что делать, если мошенники все же похитили с вашей карты денежные средства?

Как только вы это обнаружите, сразу же заблокируйте карту, а также сообщите о хищении (не позднее суток с момента получения информации о хищении необходимо написать о несогласии с операцией). Сделать это можно через мобильное приложение банка, а также позвонив в контактный-центр или обратившись в отделение банка.

Затем как можно скорее напишите заявление в полицию, лично обратившись в ближайший территориальный орган внутренних дел   
с заявлением о возбуждении уголовного дела.

В случае если вы утратили электронное средство платежа и (или) оно использовалось без вашего согласия, банк обязан в течение 30 дней возместить сумму хищения.

**Слайд 4**

Как противостоять телефонным мошенникам?

Ни в коем случае не отвечайте на звонки с незнакомых номеров. Как правило, если вам звонят с работы или из другой организации, от которой вы ожидаете звонка, вам дополнительно напишут СМС-сообщение или сообщение в мессенджере. Никогда не перезванивайте по незнакомым вам номерам.

Если разговор касается финансовых вопросов, не продолжайте разговор и положите трубку. Сотрудники банков или правоохранительных органов не запрашивают Ваши личные и финансовые данные по телефону.

Не торопитесь принимать решение, ведь мошенники добиваются именно того, чтобы вы приняли быстрое и необдуманное решение. Они используют методы социальной инженерии: торопят Вас, пугают, создают чувство паники. Не стоит поддаваться такому давлению: проверьте информацию в Интернете или обратитесь за помощью к близким родственникам.

Прежде чем принять какое-то решение, связанное с финансами, позвоните близкому человеку, в банк или в контакт-центр ведомства, сотрудником которого представлялся звонящий. Важно получить подтверждение информации именно из официального источника, контактные номера при этом берите из своей записной книжки или с официальных сайтов организаций.

Не торопитесь принимать решение: всегда лучше проконсультироваться у специалиста, которому Вы доверяете, или посоветоваться с близкими и родственниками.

Будьте бдительны и оставайтесь в безопасности!

**Слайд 5**

За 2022 год Банк России направили на блокировку информацию по более чем 756 тыс. телефонных номеров, используемых в мошеннических целях. Это выше аналогичного показателя 2021 года в 4 раза.

За I квартал 2023 года Банком России направлено на блокировку на 8 % больше номеров, чем за аналогичный период 2022 года.

В последнее время мошенники звонят через мессенджеры. При таких звонках на аватарке пользователя может быть логотип банка или организации, от имени которой он действует.

**Слайд 6**

Фишинг становится все более распространенным явлением. Фишинг – это совокупность методов, позволяющих обмануть пользователя и заставить его раскрыть свой пароль, номер банковской карты и другую конфиденциальную информацию. Чаще всего мошенники используют поддельные/фишинговые сайты.

Внешний вид таких сайтов неизменен, он совпадает с официальным сайтом, под который пытаются подделать свой сайт мошенники. Как тогда распознать фишинговый сайт?

Распознать фишиговый сайт можно по нескольким признакам: адрес сайта может отличаться от настоящего лишь парой символов; в адресной строке отсутствует https и значок закрытого замка; дизайн сайта скопирован некачественно, в текстах допущены ошибки, у сайта мало страниц или даже только одна – для ввода данных карты.

Относитесь с подозрением к письмам (сообщениям) с неизвестными ссылками и файлами для скачивания.

**Слайд 7**

Существует довольно много уловок мошенников в Интернете: например, интернет-магазины и аукционы; восстановление кредитной истории; сообщение о крупном выигрыше или выплате от государства; заманчивое предложение о работе; льготные кредиты; туристические путевки со скидкой; сбор «пожертвований» для детей, больных, животных и др.; предложения в высокодоходные инвестиции. Все они используют актуальную новостную повестку, а также воздействуют на базовые эмоции: положительные или отрицательные.

Будьте бдительны. Не верьте слепо предложениям в Интернете – проверяйте информацию на достоверность!