Повышение финансовой осознанности

Неделя повышения осведомленности населения в отношении цифрового мошенничества

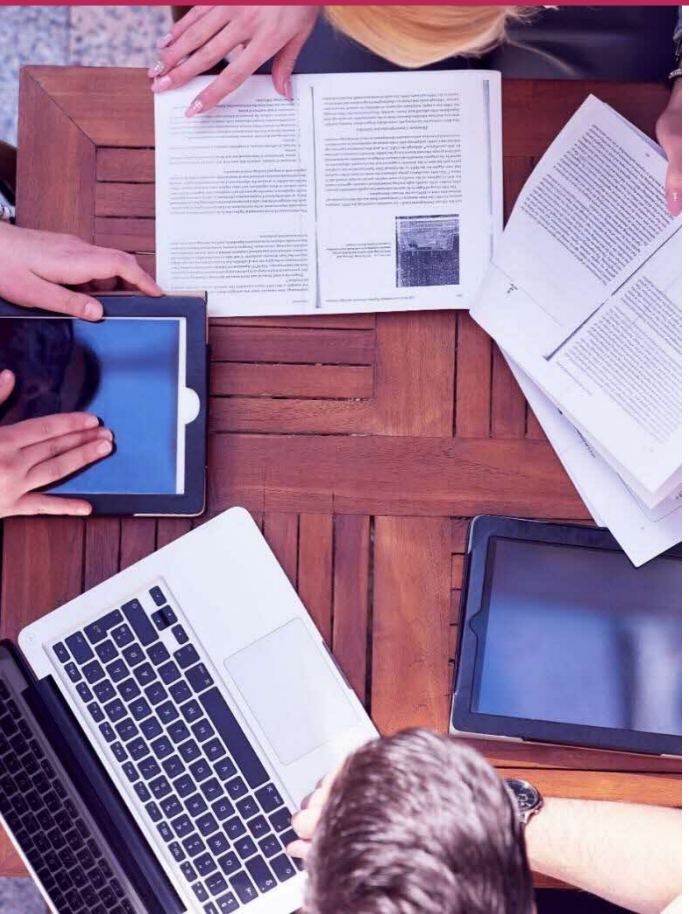
Отдел Банка Израиля по контролю за банковской системой, при участии Ассоциации банков Израиля, банковской системы и кредитных компаний

Цифровое мошенничество

Как распознать и уберечься

הגברת מודעות פיננסית

Темы встречи



- ✓ Что такое цифровое мошенничество?
- ✓ Виды мошенничества
- ✓ Как распознать?
- ✓ Как уберечься?
- ✓ Русская афера

הגברת מודעות פיננסית

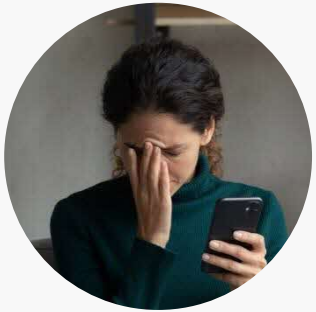
Что такое цифровое мошенничество?

- Цифровое мошенничество - это вид киберпреступления, при котором злоумышленники обманывают пользователей различными способами и крадут у них персональные данные, которые в дальнейшем используют для выполнения различных действий от их имени.
- Мошенники обращаются через смс-сообщения на мобильный телефон или звонят по телефону, с целью обманным путем получить данные авторизации для входа на банковский счет или данные кредитной карточки для произведения покупок

Почему это происходит?

Каковы причины мошенничества?

Захват профилей в соцсети



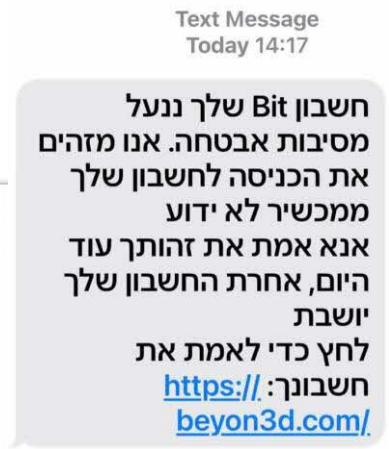
Создание помех, наблюдение или саботаж

Материальные выгоды

Получение информации

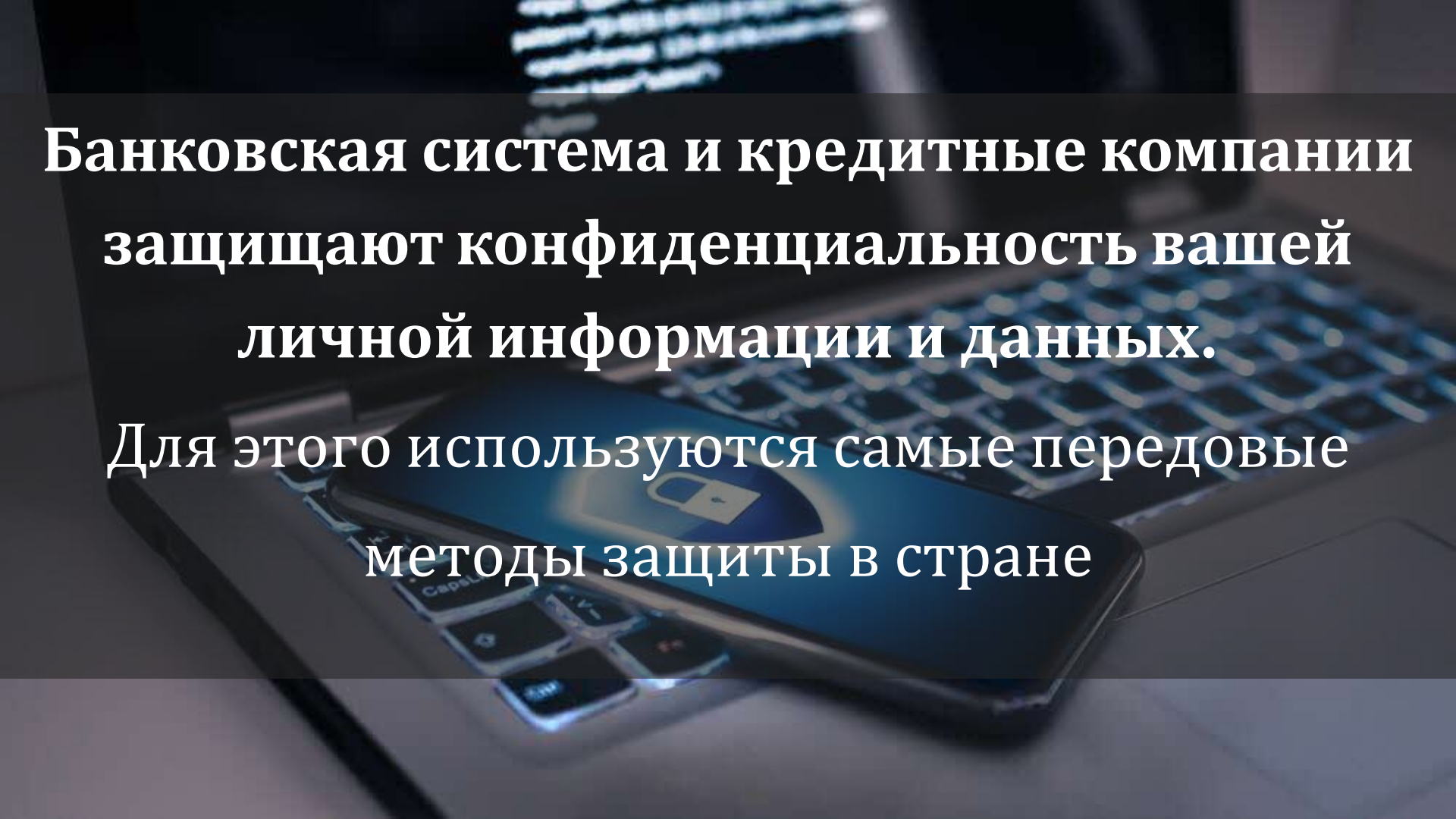
הגברת מודעות פיננסית

Как это выглядит?



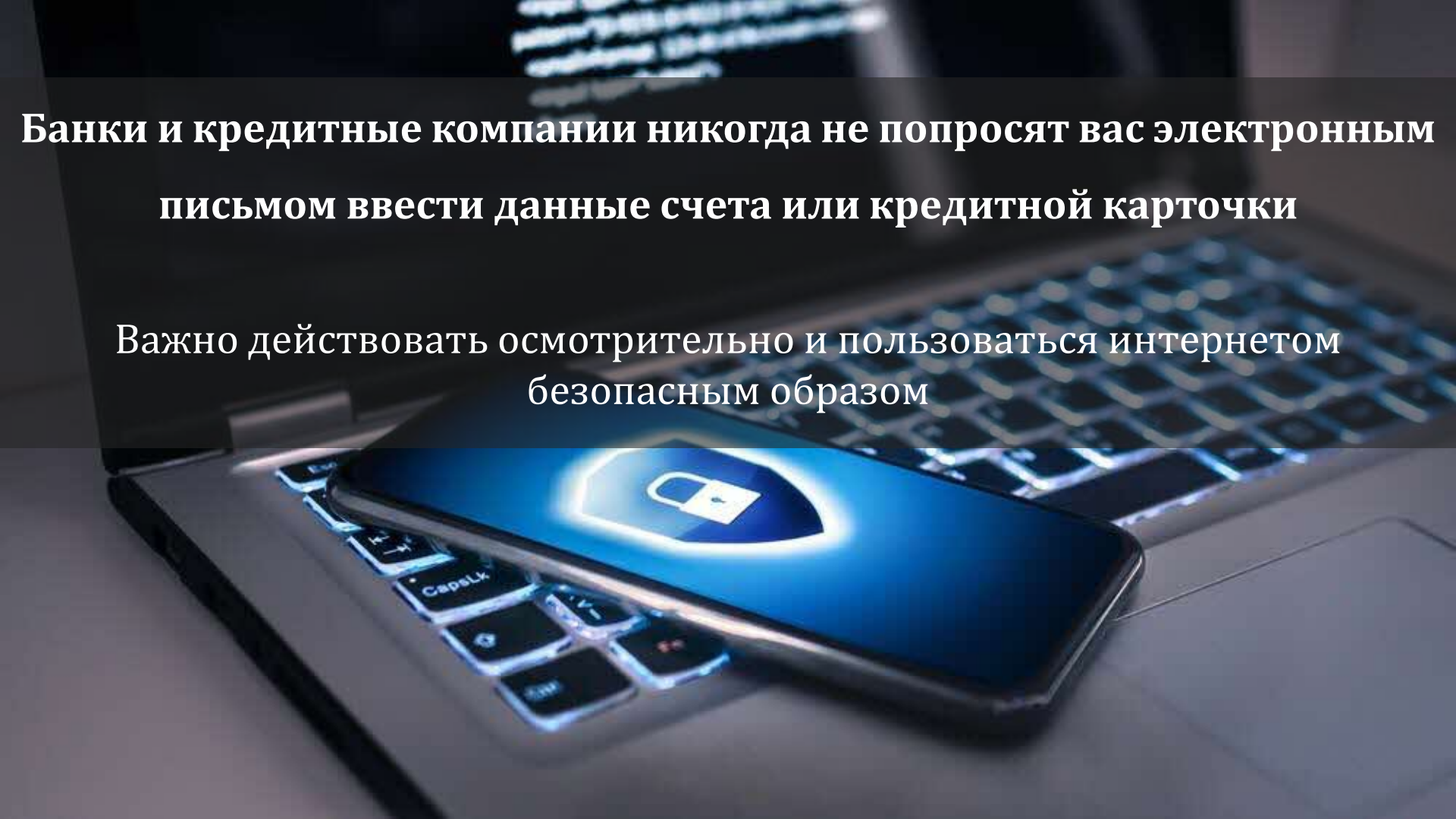
הגברת מודעות פיננסית

Кто-нибудь получал такое сообщение?



Банковская система и кредитные компании защищают конфиденциальность вашей личной информации и данных.

Для этого используются самые передовые методы защиты в стране



Банки и кредитные компании никогда не попросят вас электронным письмом ввести данные счета или кредитной карточки

Важно действовать осмотрительно и пользоваться интернетом безопасным образом

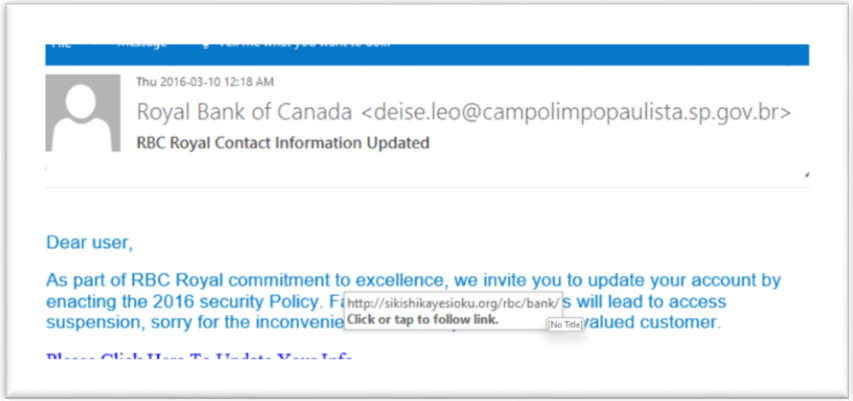
Методы

мошенничества

הגברת מודעות פיננסית

Фишинг – через электронную почту

- Фишинг - злоумышленник использует массовую рассылку и пытается «поймать в свои сети» конфиденциальную личную или финансовую информацию пользователя
- Наиболее распространенный способ - выдача себя за известный веб-сайт или финансовое учреждение
- Цель - побудить жертву заполнить поддельную форму или перейти на веб-сайт и заполнить данные авторизации/ персональные данные
- Веб-сайты могут быть очень похожи на оригинал визуально и иметь схожий URL адрес (адрес интернет-страницы веб-сайта)



Пример фишинга

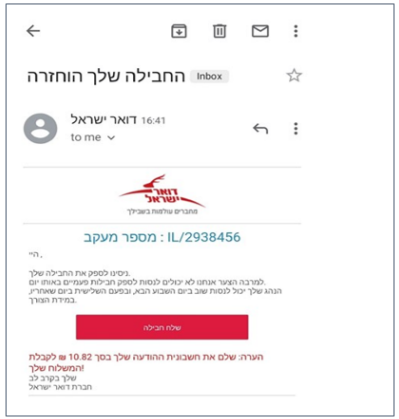
Отправка писем от имени Банка Израиля с приложением поддельных документов

Пример фишинга

Мошенничество с использованием фальшивого сообщения от Почты Израиля.
Клиент пытается заплатить определенную сумму Почте Израиля.
По факту, платеж производится на гораздо более крупную сумму и совсем другому лицу.

"להעברת תשלום בסך ILS 1075.00 באופן סופי מכרטיס 6043 לMISRADHTACHBU יש להקליד את הקוד באתר.
חשוב לדעת הקוד הוא רק שלך ואסור למסור אותו לאף אדם, לא מבית העסק ולא מחברת האשראי. אם לא ביצעת עסקה, יש לדווח מיד ל- 03-4564564

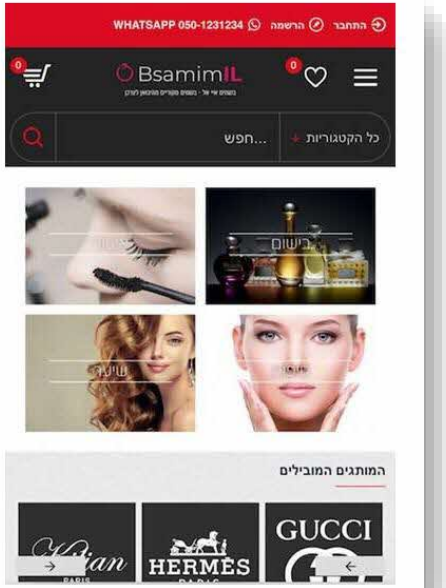
קוד האימות הוא ******..."



הגברת מודעות פיננסית

Пример фишинга

Мошенничество через кредитные карты



הגברת מודעות פיננסית

Фишинг - через смс или WhatsApp сообщение со ссылкой

- Сообщение отправляется жертве через смс или WhatsApp и содержит ссылку, предлагающую произвести легитимное действие
- Иногда, даже сам переход по ссылке дает хакеру доступ к электронному устройству
- Пример: регистрация на мероприятие, оплата, прем посылки, привлекательные скидки, скачивание приложения и прочее

Вишинг - сбор данных с помощью фальшивого телефонного звонка

Вишинг - мошенничество по телефону

- Мошенники звонят жертве и претворяются представителем законной организации, в основном по двум направлениям:
  - Полиция, служба безопасности банка или кредитной компании
  - Звонки по вопросам потребительства/инвестиций
- У вас попросят данные счета по какой-либо выдуманной причине - предупреждение, полученное на счете, маркетинговое предложение и прочее
- Имея номер телефона/удостоверения личности или пароль жертвы, злоумышленник получает возможность произвести мошенническую операцию

Фальшивый телефонный звонок «из банка»

Как может выглядеть такой разговор?

«Здравствуйте, Вас беспокоят из банка. Мы уведомляем всех клиентов о нашем приложении, чтобы Вы могли получать уведомления и льготы».

Пусть мне позвонят из моего отделения

Мы не делаем это через отделение, я только что отправил/а Вам сообщение

Окей, и что Вам от меня нужно?

Только код, который я Вам отправил/а по смс.

Фальшивый телефонный звонок «из кредитной компании»

Как может выглядеть такой разговор?

«Здравствуйте, Вас беспокоят из кредитной компании. Мы обнаружили необычные транзакции по Вашей кредитной карте».

Правда? Что там такое?

Есть необычные транзакции, превышающие обычные суммы на Вашей карточке номер 4455»

Окей, и что Вам от меня нужно?

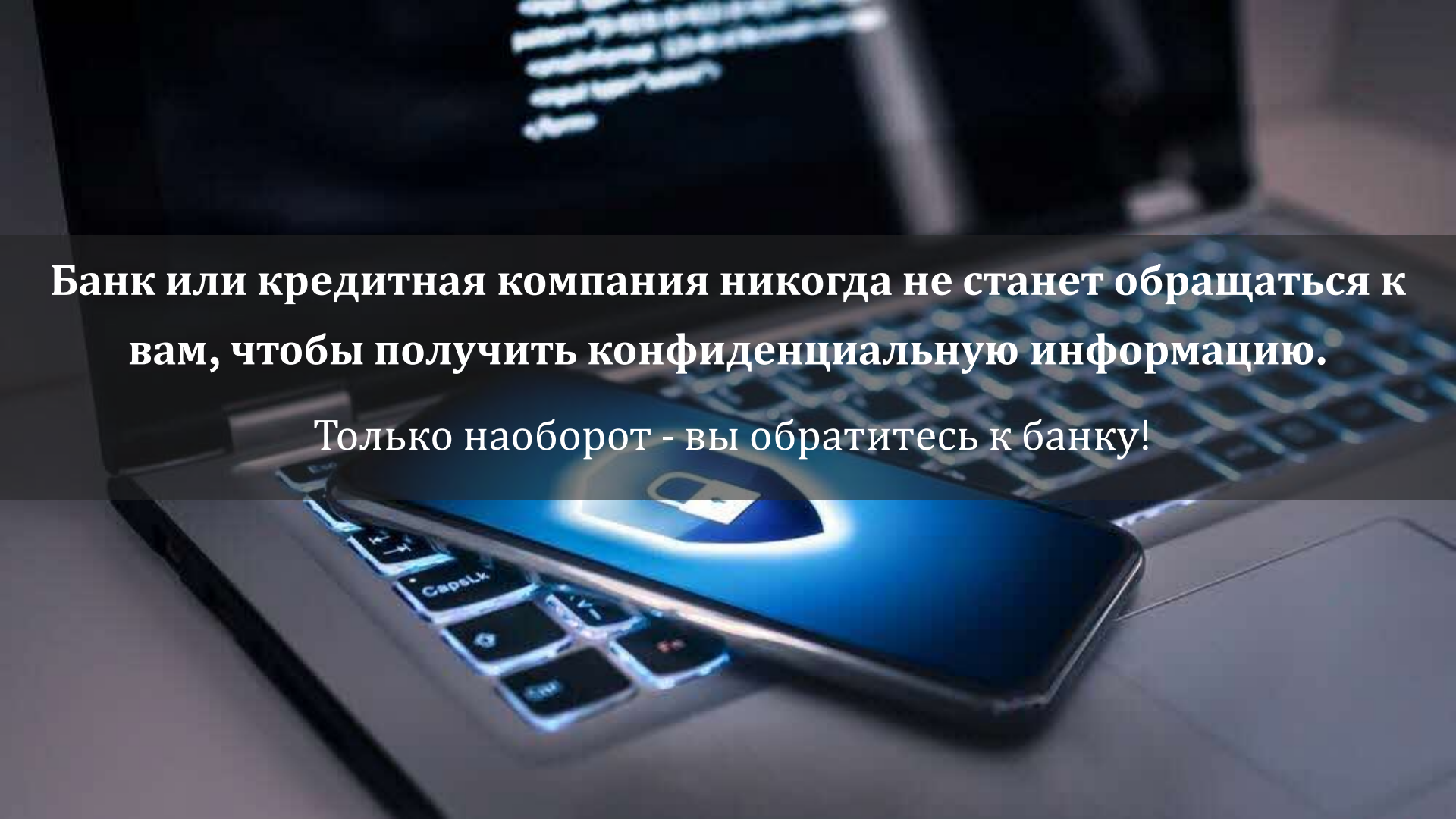
Для того чтобы остановить платежи и убедиться, что это именно Вы, мне нужен номер кредитной карты, номер удостоверения личности, а затем – код, который я Вам отправил/а.

Что бы вы сделали?

Если бы вам поступил такой звонок, как бы вы отреагировали?

1. Нужно предоставить требуемую информацию.
2. Нужно спросить, зачем им нужна эта информация и предоставить только то, что необходимо.
3. Следует отказаться предоставлять какие-либо персональные данные и положить трубку.
4. Нужно сказать, что у вас нет персональных данных, чтобы им передать, и позвонить в полицию.
5. Нужно самостоятельно позвонить в банк/кредитную компанию

הגברת מודעות פיננסית



Банк или кредитная компания никогда не станет обращаться к вам, чтобы получить конфиденциальную информацию.

Только наоборот - вы обратитесь к банку!

Как распознать?

הגברת מודעות פיננסית

Признаки, вызывающие подозрение

Обращение не является персональным

Срочность вызова

Орфографические ошибки

Выдача себя за представителя полиции

Отправка ссылки на ваш личный счет

Разговор на иностранном языке

Рекомендации к действию

- Попросите представителя говорить на иврите
- Спросите имя и должность в банке или кредитной компании
- Позвоните в банк или кредитную компанию по своей инициативе
- Не выполняйте подозрительные запросы, такие как снятие денежных средств
- Не предоставляйте данные, если Вы не являетесь инициатором разговора
- Записать номер, с которого звонили
- Сообщить в банк и подать жалобу в полицию

Давайте проверим, все ли нам ясно…

Это нормальное предложение, или нет?

Вам позвонил некто, кто представился служащим банка, и сказал, что с вашей кредитной карточки были произведены необычные платежи, и чтобы это проверить и устранить проблему вам нужно предоставить только номер вашей кредитки

הגברת מודעות פיננסית

Давайте проверим, все ли нам ясно…

Это нормальное предложение, или нет?

?

Здравствуйте, говорят из страховой компании. В рамках пакета наших услуг мы предлагаем проверить ваши страховки, чтобы избежать дублирования. Пожалуйста, скажите номер вашего удостоверения личности и данные авторизации на сайте «Хар а-кесеф», чтобы мы могли проверить ваши страховки.

הגברת מודעות פיננסית

Давайте проверим, все ли нам ясно…

Это нормальное предложение, или нет?

?

Вы получили смс-сообщение от вашего банка, в котором говориться, что возникли проблемы с вашим счетом, и вам нужно перейти по ссылке, чтобы уточнить данные вашего счета.

הגברת מודעות פיננסית

Как уберечься?

הגברת מודעות פיננסית

Как можно себя обезопасить

Не переходить по ссылкам

Использовать сильный пароль/биометрическую идентификацию

Пользоваться защищенной сетью

Скачивать приложения из официальных источников

Строго соблюдать свою конфиденциальность

הגברת מודעות פיננסית

Сильный пароль

Чего не делать

- Не используйте дату только рождения
- Не используйте только номер удостоверения личности
- Не используйте простую последовательность букв/цифр

Что делать

- Используйте комбинацию цифр и букв, которую вам легко запомнить, но которая не имеет никакого смысла для других людей
- Используйте специальные символы, такие как !@#$
- Используйте биометрическую идентификацию (сканирование отпечатка пальца/распознавание лица)

Примеры сильного пароля

- Haifa1957@#
- Zehava90210
- Batman156!

Советы, как сохранить пароль в безопасности

- Не передавайте свой пароль никому
- Не сохраняйте пароли нигде
- Ни один сайт не попросит вас озвучить пароль по телефону или в отделении - он принадлежит только вам

Не переходите по ссылкам

Не открывайте подозрительные ссылки, полученные через смс или по электронной почте от неизвестных лиц

Заведите привычку быть осторожным и осмотрительным

Если на счету есть проблема, или вам положена льгота, вы получите уведомление об этом, когда зайдете на свой счет

Скачивайте приложения из официальных источников

Скачайте официальное приложение банка/ кредитной компании из магазина приложений. Не используйте для этого ссылку

Значок магазина в гаджетах
Андроид

Значок магазина в гаджетах
iPhone

Пользуйтесь защищенной сетью

Не производите конфиденциальные операции с использованием общественной сети WI-FI

Пример незащищенных сайтов

Пользуйтесь защищенной сетью

Шаги, которые помогут нам себя защитить

- Если цены на сайте чрезвычайно низкие, или на нем указано, что ценовые предложения действуют специально для израильтян, такой сайт должен вызвать подозрения.
- Желательно проверять рекомендации и рейтинги сайтов/магазинов, прежде чем вводить платежные данные.
- Лучше производить оплату предоплаченной кредитной картой, сумма которой ограничена, или через платежные сервисы, позволяющие получить денежный возврат.
- Дайте разрешение приложению кредитной компании высылать вам уведомления о крупных транзакциях и покупках за границей/онлайн

Строго соблюдайте свою конфиденци-альность

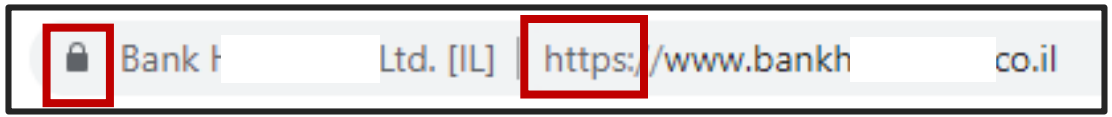
- Будьте бдительны в отношении того, что вы публикуете в сети, и желательно, чтобы ваши учетные записи в социальных сетях были закрыты для посторонних
- Не предоставляйте данные - обратите внимание, банки или кредитные компании не попросят вас указать персональные данные, такие как ваш пароль или номер кредитной карты
- Не предоставляйте данные в письменном виде / по телефону / если не вы являетесь инициатором разговора

Рекомендации по защите банковского счета и личного кабинета на сайте кредитной компании

- Предоставляйте идентификационные данные только после того, как сами перезвоните в центр обслуживания банка/кредитной компании на номер телефона, который вы сами выяснили на официальном сайте.
- Никогда не передавайте данные счета/кредитной карты, особенно, если не вы являетесь инициатором разговора.
- Вы допустили ошибку и передали данные? Незамедлительно обратитесь в банк/кредитную компанию и сообщите об этом.
- Постоянно отслеживайте банковские операции/детализацию транзакций по кредитной карте через веб-сайт или приложение, чтобы вовремя обнаружить подозрительные операции или несоответствия.
- Дайте разрешение приложению кредитной компании высылать вам уведомления о крупных транзакциях и покупках за границей/онлайн
- Если есть сомнения - нет сомнений! Лучше не ответить на сообщение, чем перейти по незащищенной ссылке.

Как зайти на цифровой счет?

1. Найдите банк или кредитную компанию X в Google или введите адрес сайта в строку поиска
2. Убедитесь, что речь идет о защищенном и надежном сайте, и что название написано



3. Используйте приложение банка/кредитной компании в своем смартфоне.

Не заходите на свой счет из полученного вами смс-сообщения или электронной почты

הגברת מודעות פיננסית

Русская афера

הגברת מודעות פיננסית

Что такое «русский обман»?

- Жертвами мошеннического метода, получившего название «русский обман», стали уже десятки пожилых людей, большинство из которых - **выходцы из бывшего СНГ**
- При этом используются специальные приложения, позволяющие **мошенникам в ходе разговора выставлять себя за служащих полиции или банка.**

הונאות פיננסיות זה לא צחוק!

הגברת מודעות פיננסית

Как производится афера?

- Мошенники используют поддельные официальные документы, такие как полицейское удостоверение / документы государственных или общественных органов, таких, как Банк Израиля
- Они используют средства оплаты без согласия жертвы и наживаются на пожилом населении обманным путем.

הגברת מודעות פיננסית

Как работает этот метод?

Здравствуйте, Тиква, говорит заместитель начальника отделения полиции. Мне жаль, но я должен Вам сообщить, что Вашим сбережениям в банке угрожает опасность.

Что значит, опасность? Что это означает?

Вы стали жертвой финансового мошенничества, Вам нужно явиться в банк и попросить пароль для медиабанка.

Никто не звонил мне из банка по этому поводу, я хочу проверить, о чем речь. Мне это кажется слишком подозрительным.

Я понимаю, это очень пугает. Но мы здесь, чтобы помочь Вам сохранить Ваши сбережения и защитить Вас. В любом случае, для начала я рекомендую не сообщать в банк, так как есть подозрение, что кто-то в банке помогает мошенникам в этой афере.

Первый этап

Звонок жертве - представление в качестве сотрудника банка/кредитной компании

הגברת מודעות פיננסית

Как работает этот метод?

После первого разговора, другой подставной представитель банка или кредитной компании звонит жертве и просит предоставить идентификационные данные, включая авторизацию для входа на банковский счет, чтобы заблокировать попытку взлома

Второй этап
Просьба предоставить данные

Жертва чувствует себя вовлеченной в процесс предотвращения мошенничества и поимки подозреваемых

הגברת מודעות פיננסית

Как работает этот метод?

Жертву просят снять наличные деньги и передать посыльному или вложить на счет менял, которые разбросаны по всей стране.

Третий этап
Перевод денег

В некоторых случаях, мошенник захватывает счет и производит перевод денег за границу, берет кредиты и прочее

Как распознать и что делать?

Как распознать	Что делать
Мошенник просит идентификационные данные	Представитель банка/кредитной компании никогда не попросит у частного клиента данные авторизации для входа на счет. Поэтому, никогда не следует передавать какие-либо данные во время входящего звонка или сообщения
Мошенник утверждает, что вы должны деньги	Проверьте документы, свидетельствующие о наличии долга.
Мошенник просит сохранить данные в тайне и не делиться ими со специалистами или членами семьи	В любом случае, посоветуйтесь с членами семьи, знакомыми служащими банка/кредитной компании, участковыми полицейскими и прочее

Лучшее лечение - это профилактика. Повышайте осведомленность о существующих способах мошенничества среди близкого окружения, и в особенности – среди членов семьи и друзей.

הגברת מודעות פיננסית

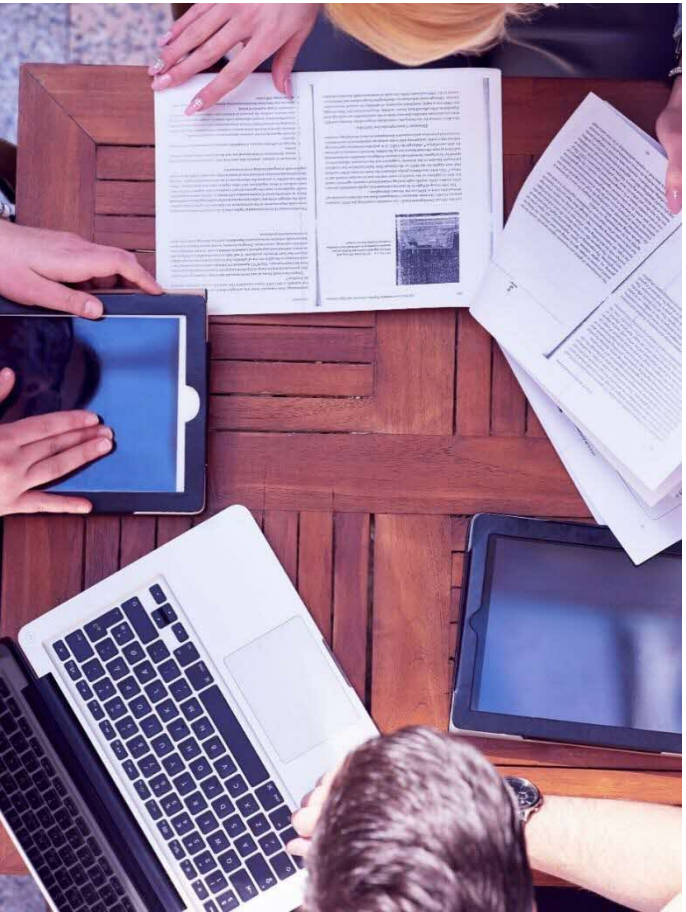
Что бы вы сделали?

Как бы вы действовали чтобы помочь родственнику не попасть в ловушку мошенников?

1. Повышение осведомленности – следует рассказывать об известных случаях мошенничества и периодически пересылать статьи и видеоролики по теме.
2. Следует взять телефон и заблокировать в нем звонки, сообщения и соцсети
3. Установить в телефоне прослушивание
4. Проверить телефон на наличие подозрительных номеров и неактуальных контактных лиц
5. Вместе проверять банковские счета, ограничить покупки онлайн и спрашивать о том, не поступали ли звонки с различными деловыми предложениями.

הגברת מודעות פיננסית

Обобщение



- ✓ Цифровое мошенничество - это один из наиболее распространенных и эффективных видов атак, используемых злоумышленниками в киберпространстве, и их число даже увеличилось в последние годы.
- ✓ Фишинг может осуществляться через электронную почту, сообщение или с помощью телефонного звонка, и призван вынудить жертву передать необходимые данные мошеннику, который выдается себя при этом за законное лицо.
- ✓ Наиболее мощным оружием мошенников является неосведомленность жертв, поэтому осознание опасности позволит вам относительно легко ее избежать.
- ✓ Воспользуйтесь советами и способами распознать мошенничество, о которых мы говорили, и сохраняйте бдительность, чтобы быть максимально защищенными.
- ✓ **Помните! Банк или кредитная компания никогда не позвонят вам и не попросят предоставить им ваши персональные данные, данные счета или кредитной карты.**

הגברת מודעות פיננסית

Есть вопросы?

הגברת מודעות פיננסית

Спасибо за внимание

הגברת מודעות פיננסית