Цифровая гигиена держателей карточек - пользователей мобильных устройств, сервисов.

НАРЦЕВА ЕЛЕНА ГЕННАДЬЕВНА

Главный специалист ОС ЦРБ

Компьютерная грамотность населения отстает от скорости внедрения новых технологий. Многие люди беспечно и формально относятся к защите и безопасности своих данных. С развитием новых технологий совершенствуются и виды мошенничества, которые строятся на психологических уловках и быстро подстраивается под стремительное появление платежных инструментов и сервисов.

По причине неосведомленности о способах совершения преступлений и излишней доверчивости многие становятся жертвами кибермошенников, а впоследствии не обращаются с заявлениями в правоохранительные органы.

ГОД	КОЛИЧЕСТВО ЗАРЕГИСТРИРОВАННЫХ **киберпреступлений** *
2020	**25,5 тысяч**
2019	**10,5 тысяч**
2018	**4741**
2017	**3033**
2016	**2471**
2015	**2440**

* МВД

Как свидетельствуют статистические данные, количество преступлений против информационной безопасности постоянно растет. И эта тенденция характерна для большинства стран мира. Количество преступлений продолжит увеличиваться в обозримом будущем в связи с активным развитием информационных технологий и растущей онлайн-зависимостью людей во всем мире. В современном мире мошенничество быстро подстраивается под стремительное развитие платежных инструментов и сервисов.

Вишинг – один из методов мошенничества, который заключается в том, что злоумышленники, используя телефонную коммуникацию (в виде звонка или СМС) и играя определенную роль, под разными предлогами выманивают у держателя платежной карты конфиденциальную информацию с целью дальнейшего хищения денежных средств.

58% звонков начинаются с сообщения о блокировке карточки (По данным ЦБ РФ)

Злоумышленники осуществляют звонки клиентам банков и представляются под вымышленным ФИО «работниками»: службы безопасности банка; службы технической поддержки; отдела рисков денежных переводов банка; службы финансового мониторинга и контроля. Реже мошенники могут представляться работниками ОАО «Банковский процессинговый центр», Ассоциации белорусских банков и Национального банка. В некоторых случаях звонящие представляются специалистами страховой компании (ЗАСО «Купала») и уточняют в каком из перечисленных банков клиент обслуживается.

Мошеннические звонки поступают в Республику Беларусь из других стран с кодами телефонных номеров, принадлежащих операторам связи Российской Федерации, Молдовы, Литвы, Эстонии. В отдельных случаях номера входящих телефонных звонков скрыты. Установлены факты использования специальных сервисов/программ-анонимайзеров, производящих подмену номера, в том числе на официальные контактные номера телефонов банков, указанные на сайте. Выявлено использование злоумышленниками схожих номеров телефонов с изменением одной либо нескольких первой(-ых) или последних цифр номера с расчетом на невнимательность клиента. Для создания большей правдоподобности в качестве шумового фона во время телефонного разговора применяется имитация звуков работающего контакт-центра.

Типичные вариации фраз, которые используют мошенники:

«С вашей картой происходят мошеннические транзакции / подозрительная активность»;
«На ваше имя поступила заявка на кредит/перевод, нужны ваши данные, чтобы отменить»;
«С вашего счета уже списали деньги, операция заблокирована, а, чтобы вернуть/ отменить или спасти то, что осталось (кстати, а сколько у вас там было?), надо все перевести на временный/единый/безопасный счет»;
«Скажите срочно код, который придет в SMS, нужно срочно аннулировать списание, иначе заблокируем карточку/ доступ в Интернет – банкинг» и т.п.

21% убеждают перевести деньги на безопасный счет
16% убеждают установить программу на устройство
(По данным ЦБ РФ)

Если Вам поступит подобный подозрительный звонок, необходимо не поддаваться на предложения сообщить информацию о реквизитах карточки, пароли и коды доступа, паспортные данные.

Прекратите разговор незамедлительно!

После разговора, самостоятельно перезвоните в банк по номерам, указанным на карточке, на официальном сайте банка, на официальных документах, выданных Банком. Важно не перезванивать по тому номеру, с которого вам позвонили. Набирать номер необходимо вручную и по возможности с другого мобильного/стационарного телефонного аппарата.

При возникновении подозрении о факте мошенничества, заблокируйте свою карточку до прояснения ситуации. Заблокировать карточку можно, позвонив в Контакт-центр Банка по номеру 147 или в круглосуточную службу сервиса клиентов ОАО «Банковский процессинговый центр» по номеру: (017) 299 25 26 или с помощью услуг SMS-банкинг, М-банкинг, или Интернет-банкинг (для карточек, зарегистрированных в данных услугах).

Храните номер телефона круглосуточной сервисной службы в удобном и всегда доступном месте на случай срочной необходимости заблокировать карточку.

Фи́шинг (от английского fishing — рыбная ловля, выуживание, термин появился 1996г.) это вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей (логинам, паролям, реквизитам карточек, номерам телефонов, паспортным данным).

Достигается как правило, путем проведения массовых рассылок электронных писем и уведомлений от имени известных брендов, банков, платежных систем, почтовых сервисов, социальных сетей. Рассылка может осуществляться через взломанные аккаунты в соц.сетях (Вконтакте, Instagram, Twitter), а также с использованием мессенджеров (Viber, WhatsApp, Telegram), в которых содержатся ссылки на нелегальный ресурс, внешне неотличимый от настоящего (официального сайта).

Киберпреступники умело маскируют поддельные интернет-ресурсы:

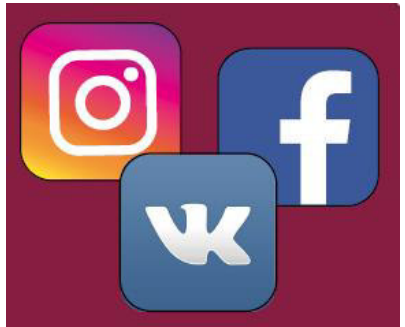
торговых интернет-площадок, служб доставки, банковских сервисов.

Приманки: выгодные акции, нереалистичные выигрыши, индивидуальные, специальные предложения, предложения просмотреть какую-то запись, пройти опрос или проголосовать, имитируется сбой системы, но при этом сайт просит ввести данные (пароли, телефоны, номер карты), чтобы якобы обновить аккаунт.

Вначале создается фишинговый сайт, полностью копирующий дизайн официального сайта. Для правдоподобности фишинговый ресурс регистрируется на доменное имя отличающееся от оригинального буквально одним символом.

Злоумышленники, чтобы усыпить бдительность жертв, могут сами оставлять на сторонних ресурсах положительные отзывы на созданный сайт. А также используя сервисы накрутки посещений сайта продвигают фальшивый ресурс в ТОПы поисковых систем.

Затем злоумышленник, связывается с потенциальной жертвой например, через мессенджеры и предлагает воспользоваться услугами сайта по сброшенной ссылке. Ничего не подозревающий Держатель карточки переходит на сайт-подделку и вводит данные своей банковской платежной карточки, тем самым отправляя их преступнику.



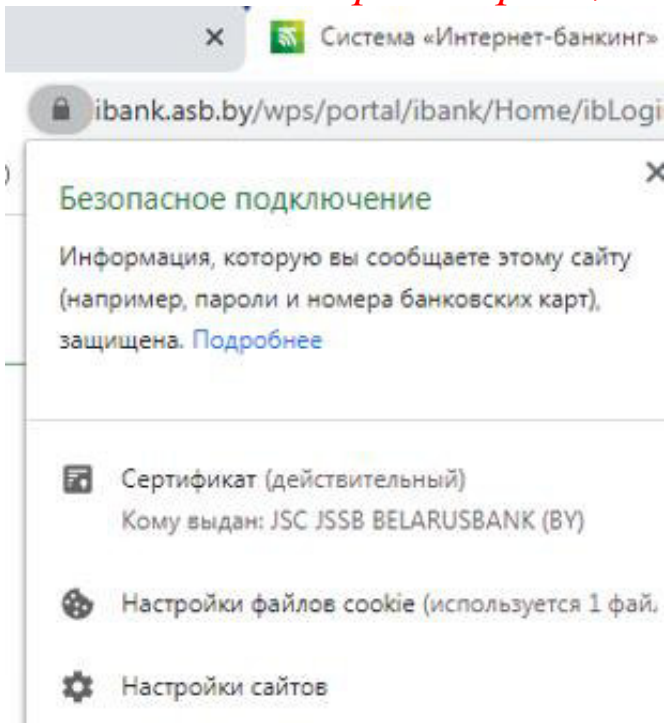
Признаки фишинговых сайтов :

Интерфейс сайта требует ввести конфиденциальные данные, в том числе, те которые никогда не вводятся

Например, *поддельный сайт Интернет-банкинга может требовать ввести номер телефона, ПИН-коды платежных карт.*

В ссылках используется **незащищенный протокол**

Всегда проверяйте, что установлено защищенное **ssl**-соединение с сайтом. В браузере адрес веб-страницы **ДОЛЖЕН** начинается с https:// с наличием пиктограммы «**закрытый замок**».



Открытый или перечеркнутый «ЗАМОК» – безопасность не подтверждена – значит нужно уйти с сомнительной страницы.

Фишинговые сайты могут скрываться за всплывающими окнами. На них может вести таргетированная реклама.

Фарминг - разновидность фишинга, при котором переход по ссылке, происходит непосредственно на официальном сайте. Фармеры меняют цифровой адрес официального сайта на DNS-сервере на адрес подменного сайта, и в результате ничего не подозревающий пользователь перенаправляется на поддельный сайт.

Используйте расширение для браузера (browser extensions, plug-in, add-on - микропрограммы для дополнения функционала), которые блокируют сомнительные и нежелательные сайты, всплывающую рекламу, перенаправление на подменные сайты, чтобы избежать предоставления доступа злоумышленников к системе, вашим паролям и данным.

Помните, что если что-то в письме /на сайте кажется подозрительным или слишком хорошим, чтобы быть правдой, то, скорее всего это обман.

Если вам кто-то пишет в мессенджере и предлагает, перейти по ссылке, не спешите это делать!

Целью фишинговой атаки может быть установка вредоносного ПО (кейлоггер, троянская программа, программа-шпион) на компьютер жертвы.

Критически и Внимательно **оценивайте** адрес сайта

Фишинговый сайт	*Оригинальный сайт*
www.21**wek**.by – **w** вместо **v** www.2**lvek**.by – **l вместо 1**	**https://21vek.by**
www.kufar.be - e вместо y www.kufarby.online	**https://kufar.by**
bellpost.be, belpost.bj, bellpochta.be	**https://belpost.by**
ewropost.by , evroposhta.by , evropost.site	**https://evropochta.by/**
www.belarusbank.fun/ www.belarusbank-vhod.ru/login.php www.24belarusbank.ru	https://belarusbank.by

Используйте только **официальные ресурсы и аккаунты** ОАО «Беларусбанка»:

Перед началом работы необходимо удостовериться в подлинности сайта!!!

Насторожить должна регистрация сайта на домене, где не существует ограничений для регистрации (например, .ru, .org, .net, .info, .biz, .top, .in, .cc, .com.ua, .in.ua, .pp.ua, .dp.ua).

на корпоративном сайте ОАО «АСБ Беларусбанк» раздел «Частым лицам / Платежные карточки / База мошеннических ресурсов Укажите сайт, который вы хотите проверить..

https://belarusbank.by/
https://vk.com/asb.belarusbank
https://www.facebook.com/asb.belarusbank
https://twitter.com/asb_belarusbank
https://ok.ru/asb.belarusbank
https://www.youtube.com/user/asbbelarusbank

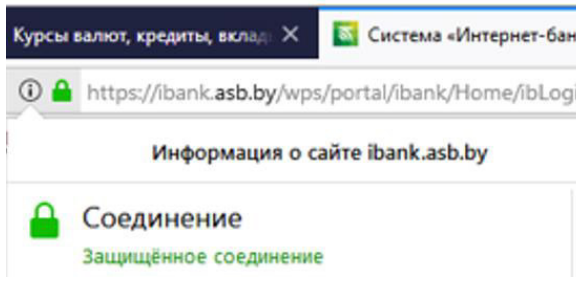
86,8 % респондентов используют интернет- банкинг (мобильный банкинг – 58,8 %).

Институтом социологии НАН Беларуси по заказу Национального банка Республики Беларусь в 2020 г. опрос населения страны

- Перед началом работы убедитесь, что на компьютере с которого производится доступ к системе «Интернет-банкинг», установлено антивирусное программное обеспечение с актуальными антивирусными базами данных.
- Не заходите на персональную страницу «Интернет-банкинг» с чужих устройств.
- Но если все-таки …, то проверять не сохранились ли ваши персональные данные на чужом устройстве.
- Не заходите в систему «Интернет-банкинг» через открытые сети Wi-Fi.

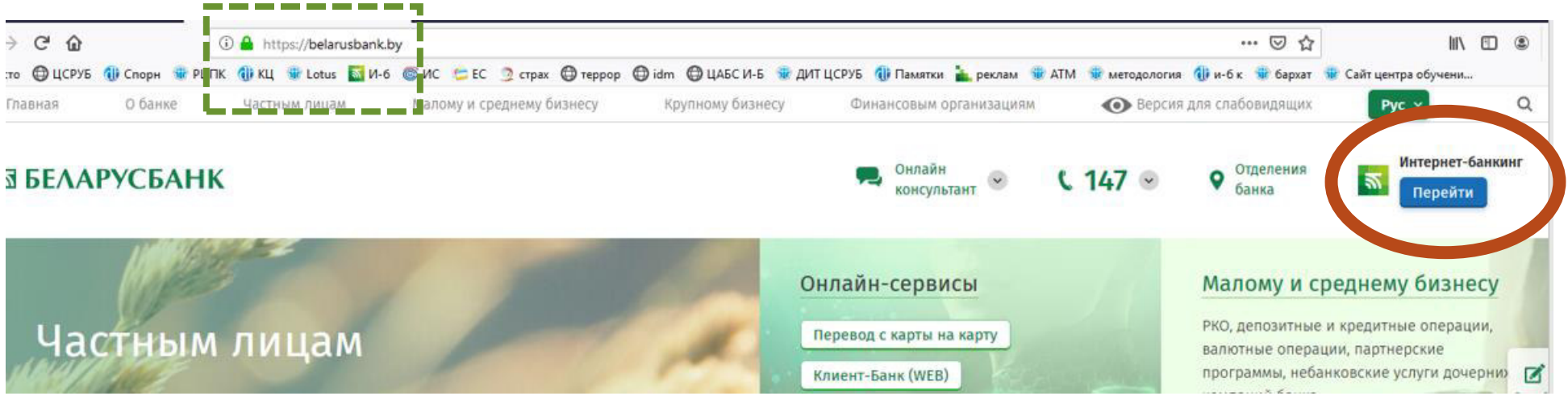
БЕЗОПАСНЫЙ Вход в систему «Интернет-банкинг»

В адресной строке интернет-браузера набрать: https://ibank.asb.by,

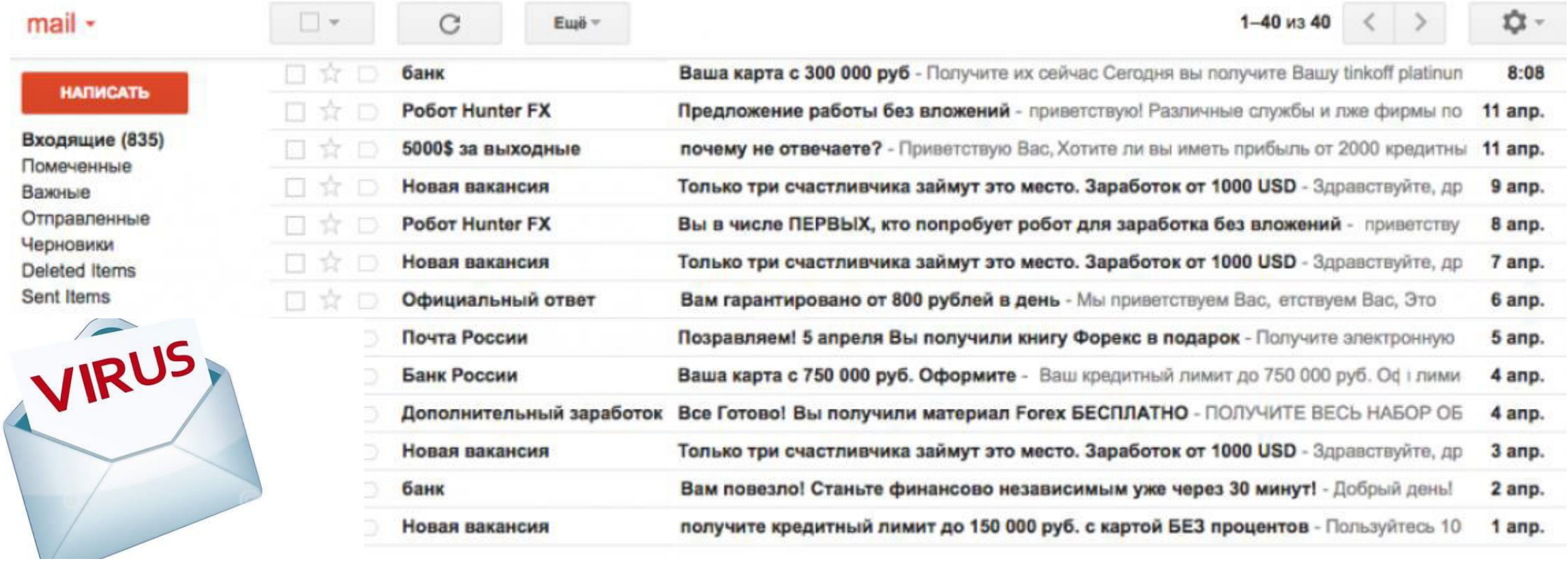


либо

адрес корпоративного веб-сайта банка:
www.belarusbank.by и перейти НАЖАТИЕМ КНОПКИ «Интернет-банкинг»



Не переходите по ссылкам и не скачивайте вложения из письма — так вы рискуете заразить компьютер вирусом, который позволит мошенникам его контролировать. И тем более не вводите данные вашей карточки.

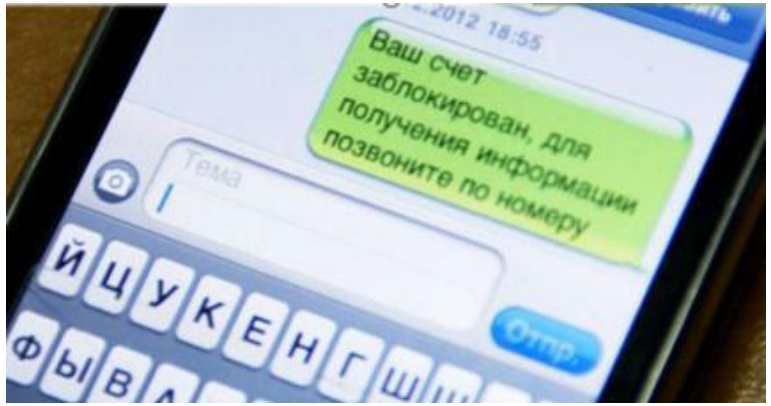


В сети Интернет злоумышленниками создана страница, на которой обещают 100 литров топлива при рассылке сообщения 20 знакомым. "Белоруснефть" такой акции НЕ ПРОВОДИТ. Информация обо всех проводимых акциях размещается на официальной сайте azs.belorusneft.by.

Мошенники пытаются заманить : предлагают работу с большой зарплатой, которую вы не искали.
Пишут, что вы выиграли машину, получили наследство от далекого родственника.
Присылают ответ на якобы ваше письмо.
Просто хотят «познакомиться поближе».

Вывод:

Работники Банка не осуществляют телефонные звонки клиентам с использованием мессенджеров (Viber, WhatsApp, Telegram) для уточнения данных паспорта, санкционирования списания денежных средств с карточек, утери карточки, о сбоях при работе с платежами, подтверждения получения/отправления перевода, о необходимости обновить персональные данные, проведения отмены операций, совершенных посредством услуг дистанционного банковского обслуживания, сети Интернет, не запрашивают коды и иную информацию, направляемую Банком на номер телефона клиента.



Банк не осуществляет рассылку SMS-сообщений, email-сообщений с предложением подтвердить, обновить персональные данные для чего нужно заполнить форму-анкету с личными данными и перейти по вложенной ссылке; с просьбой перейти по ссылке для установки какого-либо приложения (например, «AnyDesk - удаленное управление»)/обновления программного обеспечения; с просьбой принять участие в благотворительной акции путем добровольного пожертвования, а также о выигрышах денежных призов.

Не сообщайте личные, конфиденциальные, персональные, банковские данные и сведения НИКОМУ (в том числе родственникам, друзьям, знакомым, работникам банка, работникам страховой компании или представителям правоохранительных органов).

БЕЗОПАСНОЕ ИСПОЛЬЗОВАНИЕ ПРИЛОЖЕНИЙ, СОЦСЕТЕЙ И МЕССЕНДЖЕРОВ

- Ограничить список лиц со статусом «друзей» в социальных сетях. В «друзьях» не должно быть случайных и незнакомых людей;
- Закрыть доступ к своим страницам в соц.сетях людям, не входящих в круг знакомств;
- Запретить возможность добавления в группы/чаты, просматривать ваши данные людям, не входящих в список ваших контактов;
- Нельзя пересылать фотографию карточки в соц. сетях, мессенджерах.

60% преступников знают имя собеседника
42% указывают ФИО полностью

(По данным ЦБ РФ)

Если ваш аккаунт в социальных сетях был взломан, то оповестите об этом подписчиков вашей страницы, смените пароль, сообщите в службу тех. поддержки.

Особое внимание следует уделить просьбам о какой-либо помощи, связанной с передачей реквизитов карточек, логинов, паролей и пр. в социальных сетях (vk.com, ok.ru) или сервисах сообщений (Viber, WhatsApp, Telegram).

ПОЛУЧИВ СООБЩЕНИЕ ОТ РОДСТВЕННИКОВ, БЛИЗКИХ, ДРУЗЕЙ, КОЛЛЕГ ЗНАКОМЫХ– СВЯЖИТЕСЬ С ЭТИМ ЧЕЛОВЕКОМ НАПРЯМУЮ ДЛЯ УТОЧНЕНИЯ ИНФОРМАЦИИ ДЕЙСТВИТЕЛЬНО ЛИ И КАКАЯ ПОМОЩЬ НУЖНА.

Страницы в социальных сетях взламываются и со взломанных страниц осуществляется рассылка сообщений, направленных на вымогательство личных конфиденциальных данных.

➢ Использовать РАЗНЫЕ логины и УНИКАЛЬНЫЕ, СЛОЖНЫЕ пароли в своих аккаунтах в соц. сетях, приложениях, на различных сайтах, электронной почте (в помощь сервис проверки паролей);

➢ Использовать только проверенные менеджеры хранения паролей (например, Kaspersky Password Manager)

НЕЛЬЗЯ

- ❖ Создавать пароль путем набора русских слов при включенной английской раскладке;
- ❖ Использовать в качестве пароля свой логин (имя пользователя, учетная запись, никнейм), личные данные, биографическую информацию, клички животных и др. ;
- ❖ Сохранять пароль автоматически;
- ❖ Использовать повторение символов;

84%

Пользователей забывают пароль после 2 недель[3]

77%

Пользователей используют одни и те же 1-5 паролей для всех своих доступов[4]

Самые популярные пароли

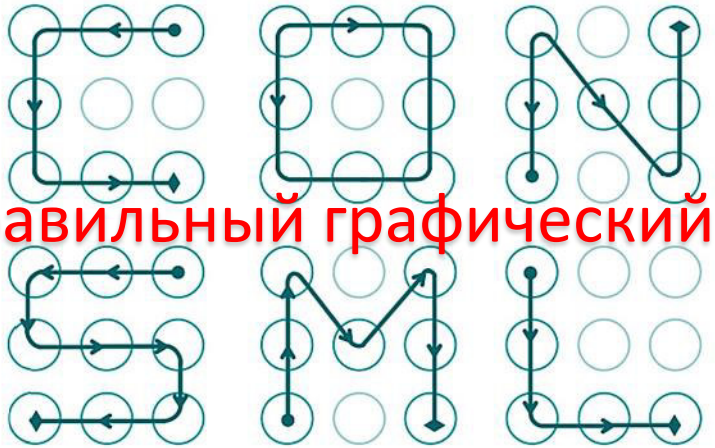
12345
qwerty
1а2б3в
пароль
откройся

Самые популярные PIN-коды

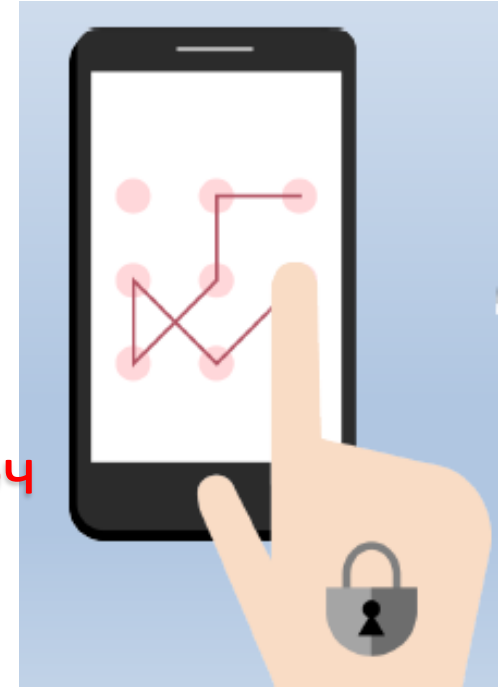
1234
1111
0000
1212
7777

Можно легко узнать

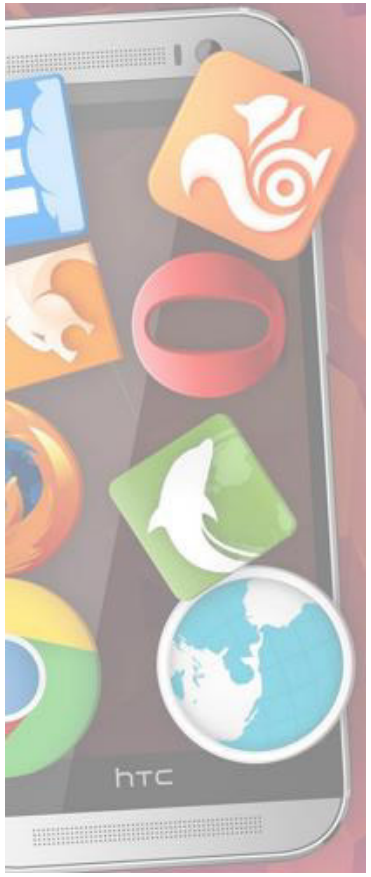
17% день рождения
10% имя
10% номер телефона
9% кличка животного



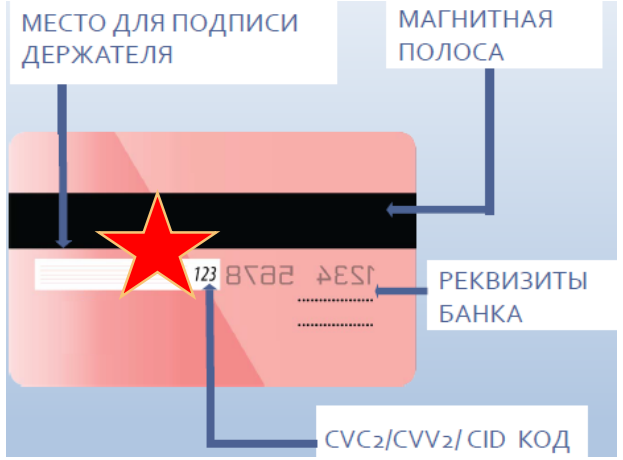
НЕ правильный графический ключ



Способы избежать взлома и хищения средств:



- Заряжая телефон через ПК выбрать функцию «ТОЛЬКО ПИТАНИЕ»;
- Деактивируйте автоматическое подключение устройства к открытым Wi-Fi точкам, не используйте общественные точки Wi-Fi; Использовать точки доступа защищенные паролем;
- Устанавливайте приложение только через ссылки, размещенные в магазинах приложений Play-Маркет, Google Play, App store с настройкой проверки на вредоносное содержание;
- Обращать внимание, к каким функциям гаджета установленные приложения запрашивают доступ;
- Использовать актуальные версии специального программного обеспечения (антивирусное), предназначенное для борьбы с вредоносной активностью, своевременно обновляйте его;
- Подключить при всех возможностях двухфакторную аутентификацию;
- Периодически проверять какие платные услуги активированы с привязкой к телефонному номеру (на планшете, смартфоне). В бесплатном контенте могут быть скрыты платные услуги и сервисы;
- НЕ ПЕРЕДАВАТЬ ВАШИ ГАДЖЕТЫ В ЧУЖИЕ РУКИ;
- Используйте QR-код-антивирус – специальную программу для смартфона, которая перед сканированием проверяет код на наличие вредоносного содержимого и предупреждает пользователя о возможной опасности.



Нельзя спешить проводить оплату, поверив заманчивым рекламным обещаниям, перепроверяйте информацию об акциях и скидках.

Чтобы не стать жертвой мошенников нужно:

- Прикрывать ладонью клавиатуру при вводе пин-кода;
- Не хранить пин-код вместе с карточкой/на карточке;
- Не сохранять в браузерах (сайтам интернет-магазинов) данные карточки для упрощения совершения платежей в будущем;
- Для онлайн-покупок/платежей оформить отдельную карту (без доступа к основному счету) и не держать на ней большие суммы;
- Нельзя сообщать CVV-код (трехзначный номер на обратной стороне) и «3-D Secure» , делать и пересылать фото карты в соц.сетях, мессенджерах и т.п;
- Скрыть CVV-код на карте, предварительно сохранив его;
- Установить лимиты для карт на суммы онлайн-операций и др. ограничения по расходованию средств;
- Подключить SMS- оповещение.

P.S. Самые опасные мошеннические схемы социальной инженерией, потому что злоумышленники атакуют не технологию, а пользователя. В большинстве случаев человек сам запускает вредоносную программу, отправляет конфиденциальные данные или подтверждает действие.