Банк России

«НАШ СОЛНЕЧНЫЙ МИР»
МИР, В КОТОРОМ ВСЕГДА ХОРОШАЯ ПОГОДА

Мошенничество

2022

Содержание

Мошенничество – это обман людей с целью украсть их деньги.

Мошенники – люди, которые пытаются обмануть вас и украсть ваши деньги.

Мошенники пытаются узнать вашу секретную информацию.

Мошенники пытаются узнать ваши личные данные.

Личные данные – это информация из ваших документов.

Мошенники хотят узнать информацию о ваших банковских счетах.

Банковский счёт – это место в банке, где хранятся ваши деньги.

Мошенники хотят узнать информацию о ваших банковских картах.

Банковская карта – это небольшая пластиковая карта, на которой хранится информация о вашем банковском счёте.

Мошенники хотят узнать ПИН-код вашей банковской карты.

ПИН-код (PIN-код) – это секретный пароль вашей банковской карты.

ПИН-код – это 4 цифры.

ПИН-код нужен, чтобы пользоваться вашей банковской картой.

ПИН-код вашей банковской карты должны знать только вы.

Не говорите, **не показывайте** и **не пишите** ПИН-код вашей банковской карты чужим людям.

Мошенники хотят узнать защитный код вашей банковской карты.

Защитный код (CVV/CVC-код) – 3 цифры на оборотной стороне вашей банковской карты.

Защитный код нужен для подтверждения платежа с вашей банковской карты.

Не говорите, **не показывайте** и **не пишите** защитный код вашей банковской карты чужим людям.

Мошенники хотят узнать одноразовый пароль из СМС-сообщения от банка.

Одноразовый пароль вы можете использовать только один раз.

Банк присылает вам пароль в СМС-сообщении на телефон.

Пароль из СМС-сообщения подтверждает платёж с вашей банковской карты.

Никому **не говорите**, **не показывайте** и **не пишите** пароль из СМС-сообщения от банка.

Мошенники обманывают людей разными способами.

Вы должны знать, как обманывают мошенники.

Тогда вы сможете защититься от мошенников.

Где мошенники могут быть опасны?

1 Мошенники могут быть опасны при использовании банкомата

Банкомат – аппарат для приёма и выдачи наличных денег.

Для использования банкомата вам нужна ваша банковская карта.

Вам нужно набрать ПИН-код вашей банковской карты.

ПИН-код – это секретный пароль вашей банковской карты.

ПИН-код — это 4 цифры.

ПИН-код вашей банковской карты должны знать только вы.

Другие люди **не должны** видеть ПИН-код вашей банковской карты.

Мошенники могут пытаться узнать ваш ПИН-код.

Мошенники могут:

- установить на банкомат специальное устройство
- установить видеокамеру над клавиатурой банкомата

Если мошенники получат информацию о вашей банковской карте, они могут украсть ваши деньги.

Если вы хотите снять деньги, внимательно осмотрите банкомат.

Если на банкомате есть лишние предметы, найдите другой банкомат.

Если клавиатура банкомата шатается, найдите другой банкомат.

Мошенники могут попытаться подсмотреть ваш ПИН-код.

Пользуйтесь банкоматом, когда рядом нет других людей.

Когда вы вводите ПИН-код вашей банковской карты, прикрывайте клавиатуру рукой.

Если вам трудно пользоваться банкоматом, попросите близкого человека помочь вам.

Если кто-то предлагает вам помощь у банкомата без вашей просьбы, откажитесь от помощи.

Если вы обращаетесь за помощью к чужим людям, будьте осторожны.

Не передавайте вашу банковскую карту чужим людям.

Не говорите, **не показывайте** и **не пишите** ПИН-код вашей банковской карты чужим людям.

Лучше пользоваться банкоматом в офисе банка.

Если вам нужна помощь, сотрудник банка поможет вам.

2 Мошенники могут быть опасны при оплате товаров и услуг в интернете

При оплате в интернете вы вводите секретную информацию:

- номер вашей банковской карты
- срок окончания действия вашей банковской карты
- ваши имя и фамилию
- защитный код (CVV/CVC-код) вашей банковской карты

Для оплаты в интернете банки присылают вам одноразовый пароль.

Одноразовый пароль вы можете использовать только один раз.

Банк присылает вам пароль в СМС-сообщении на мобильный телефон.

Одноразовый пароль нужно ввести на странице оплаты.

Пароль из СМС-сообщения подтверждает платёж с вашей банковской карты.

Чтобы получать СМС-сообщения от банка, вам нужно подключить мобильный банк.

Мобильный банк – это система, которая позволяет управлять вашими деньгами в банке с помощью СМС-сообщений.

Никому **не говорите**, **не показывайте** и **не пишите** пароль из СМС-сообщения от банка.

Никто **не должен** спрашивать у вас одноразовый пароль.

Одноразовый пароль спрашивают только мошенники.

СМС-сообщения из банка – это ваша секретная информация.

Никто **не должен** спрашивать вашу секретную информацию.

Вашу секретную информацию спрашивают только мошенники.

Иногда вам может позвонить сотрудник банка.

Он может спросить про последние платежи с вашей банковской карты.

Сотрудник банка **не должен** спрашивать у вас информацию вашей банковской карты.

Информацию банковской карты спрашивают только мошенники.

Если у вас спрашивают информацию вашей банковской карты, сразу завершите разговор.

3 Мошенники могут быть опасны в интернете

Чтобы узнать вашу секретную информацию, мошенники создают поддельные сайты.

Мошенники копируют сайты известных организаций.

Поддельный сайт очень похож на настоящий сайт организации.

Поддельный сайт имеет другой адрес в интернете.

Пример

Вы попали на поддельный сайт интернет-магазина.

Вы хотите оплатить покупку на этом сайте.

Вы вводите информацию вашей банковской карты.

Ваша секретная информация попадает к мошенникам.

Мошенники могут украсть ваши деньги.

Будьте внимательны!

Адреса поддельных сайтов очень похожи на адреса настоящих сайтов.

Пример

www.wildberries.ru – настоящий сайт интернет-магазина

www.wildberris.ru – поддельный сайт интернет-магазина

Мошенники могут прислать вам сообщение со ссылкой на поддельный сайт.

Не нажимайте на эту ссылку!

Сообщение вы можете получить:

- в телефоне
- по электронной почте
- в социальной сети

Мошенники пишут ложные сообщения.

Примеры ложных сообщений:

- ваша карта заблокирована
- с вашего банковского счёта переведены деньги
- на ваш банковский счёт зачислены деньги
- вы выиграли в лотерею
- вам нужно обновить ваши личные данные
- вам нужно подтвердить ваши личные данные

Мошенники пишут ложные сообщения, чтобы вы нажали ссылку.

Если вы нажмёте ссылку, вы попадёте на поддельный сайт.

Не нажимайте на эту ссылку!

Поддельный сайт внешне очень похож на настоящий сайт.

На поддельном сайте вас попросят ввести ваши личные данные.

Личные данные – это информация из ваших документов.

Мошенники могут украсть ваши личные данные.

Мошенники могут украсть ваши деньги.

Пример 1

Вам приходит сообщение от вашего друга.

В сообщении есть ссылка.

В сообщении говорится, что нужно нажать ссылку.

Что делать

- **не нажимайте** ссылку в сообщении
- позвоните вашему другу
- расскажите вашему другу о сообщении

Мошенники украли секретную информацию вашего друга.

Мошенники хотят украсть вашу секретную информацию.

Пример 2

Вам приходит сообщение от известного магазина.

В сообщении вам предлагают большие скидки на товары.

Вам нужно перейти на сайт по ссылке.

Чтобы получить скидку, вам нужно ввести ваши личные данные на сайте.

Что делать

- **не нажимайте** ссылку в сообщении
- найдите в интернете сайт магазина
- узнайте на этом сайте информацию о скидках

Не вводите ваши личные данные на сайте.

Известные организации никогда **не спрашивают** личные данные.

Правила безопасности:

- **не нажимайте** ссылки в неизвестных сообщениях
- **не загружайте** вложенные файлы, которые вы **не ждете**

Вложенный файл – документ, который приходит в сообщении.

Обращайте внимание на интернет-адрес в ссылке.

Обращайте внимание на адресную строку.

Интернет-адрес поддельного сайта отличается от интернет-адреса настоящего сайта.

Пример

www.wildberries.ru – настоящий сайт интернет-магазина

www.wildberris.ru – поддельный сайт интернет-магазина

Если вы постоянно пользуетесь сайтом, сохраните его в закладках.

Закладка – ссылка на сайт, которую вы сохраняете, чтобы в следующий раз сразу перейти на этот сайт.

Обращайте внимание на содержание сообщения.

Мошенники часто делают много ошибок.

Не звоните по телефонам из сообщения.

Найдите в интернете сайт организации.

На сайте организации вы можете найти номер телефона.

Позвоните по этому номеру телефона.

Вы сможете узнать нужную информацию.

Вы будете уверены, что вас **не обманули**.

Надёжно защитите ваши пароли.

Никому **не говорите** ваши пароли.

Запишите пароли на бумаге и храните в надёжном месте.

Никому **не передавайте** ваши пароли.

Никому **не говорите** и **не пишите** ваши личные данные.

Установите антивирус на ваши устройства.

Антивирус – компьютерная программа, которая защищает ваше устройство от вредных программ.

Регулярно обновляйте программы и приложения на ваших устройствах.

4 Мошенники создают финансовые пирамиды

Финансовая пирамида – это организация мошенников, которые собирают деньги с помощью обмана.

Например, мошенники предлагают людям вкладывать деньги в фонд.

Мошенники обещают очень высокий доход.

Если люди вкладывают деньги в такой фонд, мошенники украдут эти деньги.

Можно вкладывать деньги только в известные финансовые организации.

Как понять, что вас обманывают?

Как понять, что вас зовут в финансовую пирамиду?

Признаки финансовой пирамиды:

- вам обещают высокий доход
- вам говорят, что нет никаких рисков
- вас просят внести деньги сразу
- вас просят внести наличные деньги
- вас просят привести друга

На финансовых пирамидах заработать нельзя.

Мошенники заберут ваши деньги.

Вы **не сможете** вернуть ваши деньги.

5 Мошенники бывают на торговых сайтах

В интернете есть торговые сайты.

На этих сайтах вы можете сами продавать и покупать товары.

На торговых сайтах вы можете встретить мошенников.

Будьте внимательны.

Мошенники могут вас обмануть.

Пример 1

Вы хотите купить товар.

Продавец товара живёт в другом городе.

Товар нужно переслать в ваш город.

Продавец требует заранее оплатить пересылку товара.

Продавец просит перевести деньги на его банковскую карту.

Что делать

- **не переводите** деньги заранее
- вы **не получите** товар
- вы потеряете деньги

Платите деньги после того, как получите товар.

Если продавец требует заранее заплатить ему деньги, **не общайтесь** с ним.

Найдите другого продавца.

Пример 2

Вы хотите что-то продать.

Покупатель хочет перевести деньги на ваш банковский счёт.

Покупатель просит у вас номер вашей банковской карты.

Покупатель просит у вас защитный код (CVV/CVC-код) вашей банковской карты.

Что делать

Защитный код банковской карты (CVV/CVC-код) – это секретный код.

Никому **не говорите** и **не пишите** защитный код вашей банковской карты.

Чтобы перевести вам деньги, покупателю нужен только номер вашей банковской карты.

Если покупатель просит вашу секретную информацию, **не общайтесь** с ним.

Пример 3

Вы разместили объявление о продаже товара.

Вы получаете СМС-сообщение с неизвестного номера.

В сообщении вы можете прочитать ложную информацию:

- ваше объявление заблокировано за нарушение правил
- есть отклик на ваше объявление
- пришлите СМС с кодом для отмены блокировки

Что делать

Не отправляйте СМС-сообщение на неизвестный номер.

Вы можете потерять много денег.

Зайдите на сайт, где вы разместили объявление.

Найдите на сайте контакты службы поддержки.

Напишите или позвоните в службу поддержки сайта.

Расскажите о сообщении, которое вы получили.

Вам скажут, что нужно делать.

6 Мошенники могут присылать электронные письма

Мошенники могут присылать вам письма на электронную почту.

Мошенники могут предлагать вам:

- много денег за помощь
- пройти опрос
- получить приз

Не верьте тем, кто предлагает вам деньги и призы.

Не отвечайте на письма от незнакомых людей.

Пример 1

Вы получаете электронное письмо.

Незнакомый человек просит вас помочь получить наследство.

Человек обещает вам за помощь много денег.

Что делать

Сразу удалите письмо.

Не верьте тем, кто предлагает вам много денег.

Если вы согласитесь помогать, вы потеряете много денег.

Пример 2

Вы получаете электронное письмо.

В письме вам предлагают пройти опрос.

Вам обещают выдать приз.

Чтобы получить приз, нужно заплатить деньги.

Что делать

Не платите деньги.

Если опрос настоящий, вам **не нужно** платить деньги.

Только мошенники просят заранее платить деньги.

7 Мошенники могут предлагать вам работу

В интернете вам предлагают устроиться на работу.

Вам предлагают большую зарплату.

Вас просят заранее оплатить услуги по устройству на работу:

- вы должны оплатить оформление документов
- вы должны оплатить пропуск на территорию организации
- вы должны купить обучающие материалы
- вы должны заплатить за обучение

Не надо платить.

Вы потеряете ваши деньги.

Вы **не получите** работу.

Помните!

Организации **не берут** деньги у будущих работников.

Только мошенники просят заплатить при устройстве на работу.

Чтобы устроиться на настоящую работу:

- вам **не нужно** платить за обучение
- вам **не нужно** покупать продукцию
- вам **не нужно** платить за трудоустройство

8 Мошенники могут говорить, что они представители банков и государственных организаций

Мошенник может представиться сотрудником вашего банка.

Мошенник может представиться сотрудником государственной организации.

Мошенники могут позвонить вам по телефону.

Мошенники могут прийти к вам домой.

Мошенники подделывают официальные документы, чтобы вы им поверили.

Будьте внимательны!

Не верьте незнакомым людям, если они звонят вам и что-то спрашивают.

Не открывайте дверь незнакомым людям!

Пример 1

Вы получаете СМС-сообщение.

В сообщении написано, что ваша банковская карта заблокирована.

Если банковская карта заблокирована, она **не работает**.

В сообщении есть номер телефона.

Вам предлагают позвонить в банк по этому номеру телефона.

Вы звоните по этому номеру.

Вам отвечают мошенники.

Мошенники спрашивают у вас информацию вашей банковской карты.

Что делать

Никому **не говорите** информацию вашей банковской карты.

Не звоните по номеру телефона в сообщении.

Позвоните в банк.

Номер телефона банка есть на вашей банковской карте.

Спросите у сотрудника банка, что случилось с вашей банковской картой.

Сотрудник банка поможет вам.

Пример 2

К вам домой приходит человек.

Человек говорит, что он социальный работник.

Он рассказывает вам про новый прибор.

Человек говорит, что этот прибор дорого стоит.

Он предлагает вам купить прибор за небольшие деньги.

Что делать

Не покупайте ничего у чужих людей, которые пришли к вам домой.

Вы потеряете ваши деньги.

Не пускайте чужих людей в дом, если вы их **не приглашали**.

Чужие люди могут обмануть вас.

Чужие люди могут украсть у вас деньги и вещи.

Правила безопасности

Когда вы пользуетесь банковской картой:

- **не оставляйте** вашу банковскую карту без присмотра
- **не передавайте** никому вашу банковскую карту
- никому **не говорите**, **не показывайте** и **не пишите** ПИН-код вашей банковской карты
- никому **не сообщайте** информацию, которую вы получили от банка

Сотрудник банка **не имеет права** спрашивать вашу секретную информацию.

Вашу секретную информацию спрашивают только мошенники.

При любых проблемах с вашей банковской картой срочно звоните в банк.

Телефон банка есть на обороте вашей банковской карты.

Телефон банка вы можете найти на сайте вашего банка.

Используйте банкоматы в безопасных местах.

Не открывайте файлы и ссылки из незнакомых источников.

Установите антивирус на ваших устройствах.

Антивирус – компьютерная программа, которая защищает ваше устройство от вредных программ.

Когда вы пользуетесь интернетом, **не пользуйтесь** публичным Wi-Fi.

Wi-Fi – это беспроводной интернет.

Публичный Wi-Fi – это беспроводной интернет в общественном месте.

Пользуйтесь только безопасными сайтами.

Адрес безопасного сайта начинается так:

https://

В адресной строке безопасного сайта вы увидите значок в виде замка:

Знак безопасного сайта

Загружайте приложения для смартфона только с официальных сайтов.

Приложение с другого сайта может содержать вредные программы.

Будьте внимательны, когда загружаете банковские приложения на смартфон.

Обращайте внимание, кто создал банковское приложение.

Официальные банковские приложения создаёт сам банк.

Не загружайте приложения от других организаций.

Оплачивайте покупки только на сайтах с защищённым соединением.

На этих сайтах должен быть значок платёжной системы вашей банковской карты.

Если на сайте нужно ввести ваши личные данные, будьте осторожны.

Если вам звонят незнакомые люди.

Будьте внимательны! Проверяйте информацию.

Позвоните в организацию по официальному номеру телефона.

Номер телефона вы можете найти на сайте организации.

Если вам сообщили о блокировке банковской карты, позвоните в ваш банк.

Спросите у сотрудника банка, что случилось с вашей банковской картой.

Телефон банка есть на обратной стороне вашей банковской карты.

Телефон банка вы можете найти на сайте банка.

Адрес сайта банка вы можете найти на сайте Банка России:
http://cbr.ru/banking_sector/credit/FullCoList

Никогда **не спешите** платить деньги.

Спокойно подумайте.

Посоветуйтесь с близким человеком.

Если вас обманули, сразу обратитесь в полицию.

Словарь

Антивирус – компьютерная программа, которая защищает ваше устройство от вредных программ.

Банковская карта – это небольшая пластиковая карта, на которой хранится информация о вашем банковском счёте.

Банковская карта позволяет вам пользоваться деньгами с вашего банковского счёта.

Банковский счёт – это место в банке, где хранятся ваши деньги.

Банкомат – аппарат для приёма и выдачи наличных денег.

Вложенный файл – документ, который приходит в сообщении.

Закладка – ссылка на сайт, которую вы сохраняете, чтобы в следующий раз сразу перейти на этот сайт.

Защитный код (CVV/CVC-код) — 3 цифры на оборотной стороне вашей банковской карты.

Личные данные – это информация из ваших документов.

Мобильный банк – это способ управления вашим банковским счетом через СМС-сообщения.

Мошенники – люди, которые пытаются обмануть вас и украсть ваши деньги.

Мошенничество – обман людей с целью украсть их деньги.

Одноразовый пароль вы можете использовать только один раз.

Пароль из СМС-сообщения подтверждает платёж с вашей банковской карты.

ПИН-код (PIN-код) – это секретный пароль банковской карты.

ПИН-код нужен, чтобы пользоваться банковской картой.

ПИН-код – это 4 цифры.

ПИН-код вашей банковской карты должны знать только вы.

Поддельный сайт очень похож на настоящий сайт организации, но имеет другой адрес в интернете.

Поддельные сайты создают мошенники.

Публичный Wi-Fi – беспроводной интернет в общественном месте.

СМС-сообщение (СМС) – это текстовое сообщение в мобильном телефоне.

Финансовая пирамида – это организация мошенников, которые собирают деньги с помощью обмана.

Wi-Fi – это беспроводной интернет.

Запомните!

Не бойтесь просить помощи, если вы в чём-то не уверены.

Кто может помочь вам понять финансовые вопросы?

Куда вы можете обратиться за дополнительной информацией?

Вы можете получить помощь и узнать ответы на ваши вопросы здесь:

- **Ваша семья и ваши друзья**
- **Ваш банк**
  Вы можете написать свои вопросы на сайте банка.
  Вы можете позвонить в ваш банк по телефону. Контактные данные вы можете найти на сайте банка в интернете.
  Вы можете прийти в офис банка и задать вопросы сотруднику банка.

Банк России

Вы можете задать вопрос в чате мобильного приложения «ЦБ онлайн».

Вы можете позвонить по телефону:
8-800-300-30-00

АНО «Наш Солнечный Мир»

Вы можете прислать вопросы по электронной почте: info@solnechnymir.ru

Сайт «Финансовая культура»:
www.fincult.info/feedback

Вы можете найти ответ на ваш вопрос
на этом сайте.
Вы можете написать вопрос на этом сайте.

ПОЛИЦИЯ РОССИИ НАПОМИНАЕТ!

ПЕНСИОНЕРЫ,
ИНВАЛИДЫ, ВЕТЕРАНЫ
И РОДИТЕЛИ НЕСОВЕРШЕННОЛЕТНИХ,

ЭТА ПАМЯТКА – ДЛЯ ВАС!

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОЛИЦИЯ РОССИИ НАПОМИНАЕТ!

ПЕНСИОНЕРЫ,
ИНВАЛИДЫ, ВЕТЕРАНЫ
И РОДИТЕЛИ НЕСОВЕРШЕННОЛЕТНИХ,

ЭТА ПАМЯТКА – ДЛЯ ВАС!

СЛУЖА ЗАКОНУ – СЛУЖИМ НАРОДУ!

Оглавление

Уважаемые граждане!

С помощью этой брошюры полиция России обращается к вам в связи с участившимися случаями попыток мошенничества.

Отвергая нормы морали и права, мошенники стремятся похитить сбережения и ценности граждан. Их жертвами чаще становятся те, кто живет или подолгу остается в квартире один и не может за себя постоять. Это оставленные дома без присмотра дети, инвалиды, одинокие граждане, пенсионеры и люди старшего возраста.

Специально разработанное полицией руководство поможет вам обезопасить себя и своих близких. Возьмите нашу Памятку с собой, отдайте ее родителям, пожилым соседям, обучите перечисленным здесь правилам детей.

Соблюдение этих простых правил – ВАШ ВКЛАД В БЕЗОПАСНОСТЬ как вашего дома и имущества, так и ваших друзей и родных!

Помните: предупрежден – значит вооружен!

ВАШ ДОМ – ВАША КРЕПОСТЬ!

- **Правило 1.** Не открывайте дверь незнакомцам! Если вы не можете рассмотреть лицо или документы посетителя в глазок – накиньте цепочку, перед тем как отпирать замок!

- **Правило 2.** Если при исправном дверном глазке после звонка в дверь пропал обзор (глазок заклеен или закрыт) – не открывайте дверь! Громко сообщите, что звоните в полицию, - и немедленно сделайте это! (См. стр. 22.)

- **Правило 3.** Без проверки не впускайте в квартиру посторонних, даже если они представляются сотрудниками ремонтных служб. Прочитайте удостоверение и проверьте полномочия сотрудника, позвонив в приславшую его организацию! (См. стр. 22.)

- **Правило 4.** Если вам нужно впустить постороннего в квартиру, сразу заприте за ним дверь, чтобы никто не мог зайти следом. Не оставляйте ключ в двери или опустите собачку замка, чтобы ваш гость не мог впустить за вашей спиной кого-то еще. НЕ ВЫПУСКАЙТЕ ИЗ ВИДА человека, которого вы впервые впустили в квартиру!

- **Правило 5.** Не принимайте на веру то, что говорят вам пришедшие к вашей двери незнакомцы. Даже крик «Пожар!» или «Помогите!» может быть приманкой! Если при взгляде в глазок вы не заметите признаков задымления или явно совершаемого преступления – оставайтесь дома и вызывайте помощь по телефону (См. стр. 22.)

Главное правило: всегда держите данную Памятку со всеми необходимыми номерами телефонов под рукой. Если к вам в дом пытаются проникнуть против вашей воли – СРАЗУ ЖЕ ЗВОНИТЕ В ПОЛИЦИЮ! ВАМ ОБЯЗАТЕЛЬНО ПОМОГУТ!

ДОВЕРЯЙ, НО ПРОВЕРЯЙ!

Помните: нельзя узнать человека за минуту. Не слишком доверяйте тем, кого видите впервые!

- Если социальные работники, контролеры службы газа, слесари, электрики или представители жилищно-эксплуатационной конторы **пришли к вам без вызова**, это повод насторожиться!
- Мошенники часто выдают себя за представителей сферы обслуживания. **Униформа и инструменты мало о чем говорят**. Если вы не знаете человека в лицо, проверьте его документы или спросите, в какой организации он работает.
- До того как открыть дверь незнакомцу, **позвоните в названную им организацию** и уточните, направляли ли оттуда к вам специалиста. Не стесняйтесь – **это совершенно нормально!**
- Проверьте номер телефона, который вам называет сотрудник. Не звоните с его мобильного

телефона или под диктовку, набирайте номер сами. **Запишите все нужные телефоны заранее – прямо в эту Памятку!** (См. стр. 22.) Все телефоны социальных служб можно узнать в единой бесплатной справочной службе **09.**

- Если ремонтник сообщает вам о поломке и предлагает приобрести что-либо для ее устранения, стоит проверить цену на запасные части и услуги по замене, **обратившись по телефону в диспетчерскую!**

- Проверяйте платежные документы, которые кладут вам в почтовый ящик. **Известны случаи вброса фальшивых квитанций.** Если вы их оплатите, то деньги получат мошенники! Реквизиты (платежные номера) в квитанции должны совпадать с теми, по которым вы платили ранее. Если что-то выглядит не так, как обычно, обратитесь в обслуживающую ваш дом фирму и узнайте, менялись ли реквизиты! (См. стр. 22.)

ОЧЕНЬ ВАЖНО! Прежде чем принять любое решение, связанное со значительными расходами, **обязательно посоветуйтесь с близкими!**

НЕ ВЕРЬТЕ ТЕМ, КТО ОБЕЩАЕТ ЧУДЕСА ЗА ДЕНЬГИ!

Каждого из нас с детства учат быть добрым и отзывчивым. Это правильно, но в наши дни не стоит быть чересчур доверчивым! Вот ситуации, которые **должны вас насторожить**:

- Вам позвонили в дверь, но **когда вы подошли к глазку – за ним темнота или несколько незнакомых людей** на площадке у двери соседа. Это могут быть воры! Понаблюдайте за ними: в случае если подозрение подтвердится – звоните в полицию!

- Незнакомцы просят у вас помощи: воды, лекарство, позвонить, говорят, что в подъезде кто-то рожает, кому-то плохо с сердцем и так далее. **Оказать самую ценную помощь** – передать воду, таблетку или вызвать «скорую» **вы можете, не снимая цепочки с двери!**

- **Вам звонят по телефону или в дверь, заботливо уговаривают или, наоборот, запугивают болезнями и бедами.** Гости предлагают приобрести чудодейственные препараты, еду, технику, что-то еще,

часто неправдоподобное: гадания, волшебное излечение, омоложение, приворот на удачу.

ПОМНИТЕ: до покупки любых препаратов, особенно дорогостоящих, обязательно посоветуйтесь с лечащим врачом и родственниками!

У МЕНЯ ЗАЗВОНИЛ ТЕЛЕФОН...

Телефоны, компьютеры и электронные архивы позволяют узнать о вас довольно много. Не дайте ввести себя в заблуждение. **Если к вам звонят или приходят незнакомые люди, которые что-то знают о вас**, скорее всего – ЭТО МОШЕННИКИ. Вот ситуации, которые ДОЛЖНЫ ВАС НАСТОРОЖИТЬ:

- Вам звонят якобы из поликлиники и сообщают, что у вас или ваших родственников обнаружили опасную болезнь. Вне зависимости от сложности «спектакля» жуликов (могут упоминаться ваша история болезни, имя родственника, фамилия участкового врача) это – мошенничество! **Настоящий доктор никогда не сообщит такие «новости» по телефону!** Рано или поздно мошенники скажут, что только их дорогое лекарство или операция могут помочь. **НЕ ВЕРЬТЕ! ЭТО ОБМАН!**
- **Вам звонят с сообщением, что ваш родственник или знакомый попал в аварию, за решетку,**

в больницу, и теперь за него нужно внести залог, штраф, взятку – в общем, откупиться. **ЭТО ЖУЛИКИ!** Техника сегодня позволяет даже подделать голос человека.

- На телефон поступают **звонки или сообщения с неизвестных номеров** с просьбой положить на счет деньги, чтобы помочь детям или получить якобы выигранный приз. **ЭТО ЛОЖЬ!**
- Вам сообщают о крупном денежном или вещевом выигрыше по SMS и **предлагают отправить SMS-сообщение или позвонить** по указанному номеру для получения приза. **НЕ ДЕЛАЙТЕ ЭТОГО! ЭТО, КАК ПРАВИЛО, МОШЕННИЧЕСТВО.**

БУДЬТЕ БДИТЕЛЬНЫ, СПОКОЙНЫ И НЕ БОЙТЕСЬ ЗАПУГИВАНИЙ И УГРОЗ! ОБЯЗАТЕЛЬНО СВЯЖИТЕСЬ С РОДСТВЕННИКАМИ!

БЕСПЛАТНЫЙ СЫР – В МЫШЕЛОВКЕ!

Сегодня люди, особенно пенсионеры, бывают стеснены в средствах. Бессовестные жулики стараются нажиться и на этом, отбирая у стариков последнее. Вот ситуации, которые ДОЛЖНЫ ВАС НАСТОРОЖИТЬ:

- **Незнакомец представляется социальным работником** и сообщает о надбавке к пенсии, перерасчете квартплаты, премии ветеранам, срочном обмене денег на дому, якобы «только для пенсионеров». **Каким бы любезным и участливым ни был этот человек – ЭТО МОШЕННИК!**

- Любые **выплаты пенсионерам осуществляются ТОЛЬКО прикрепленным социальным работником** и вы, скорее всего, знакомы с ним. Без официального объявления в нашей стране не может проводиться никакой «срочный обмен денег»!

- **Незнакомые люди предлагают вам приобрести продукты или товары по неправдоподобно низким «льготным» ценам.** Вам могут даже продать пакет сахара или гречки за несколько рублей. **ЭТО ЛОВУШКА!** Вскоре вас попросят написать список нужных вам продуктов и попытаются взять крупный задаток. **Это выманивание денег!**

- Люди официального вида с бумагами в руках просят вас под расписку, «для выставки в музее» или под другим предлогом, **отдать им ваши ордена, боевые медали, китель или наградное оружие. ЭТО ОХОТНИКИ ЗА НАГРАДАМИ!**

- **Вам предлагают необычайно «прибыльное» предприятие:** приз, суперскидку, выгодное вложение средств, спор на деньги и т. п. Вас могут запугивать или подначивать, обещая при этом барыши. **ЭТО ОБМАН!**

НА ВСЯКИЙ СЛУЧАЙ!

Если вы ВСЕГДА соблюдаете рекомендации, приведенные в этой брошюре, вам, скорее всего, бояться нечего: жулики отправятся искать добычу полегче. Полиция России просит вас обратить внимание еще на ряд рекомендаций:

- **Познакомьтесь и дружите с соседями!** Они всегда могут прийти на выручку. Если вы знаете соседей в лицо, незнакомый человек на площадке – повод насторожиться.

- **Запишите на последних страницах Памятки** все необходимые номера телефонов. **Не стесняйтесь звонить по инстанциям!** Храните Памятку рядом с телефонным аппаратом!

- Если вы впустили кого-то в квартиру, постарайтесь, чтобы он не прошел дальше коридора. **Чем меньше посторонние находятся у вас дома, тем меньше вы рискуете!**

- **Если на улице с вами пытается заговорить незнакомец,** обращаясь к вам с просьбой, вопросом или предложением, будьте бдительны! Этот милый человек может оказаться мошенником, который, усыпив вашу бдительность, обманным путем присвоит ваши деньги и прочее имущество, а вы узнаете, что стали жертвой мошенника, только оказавшись дома.

- Если что-либо из предлагаемого вам или происходящего с вами вызывает сомнения – насторожитесь. Посоветуйтесь с детьми, родственниками, официальными органами. **НИКОГДА и НИКОМУ не отдавайте свои сбережения и документы!**

- Не все, кто разговаривает с вами участливо и убедительно, на самом деле желают вам добра. **Мошенники умеют втираться в доверие** и могут даже пытаться устраиваться на работу в соцслужбы! Если предложение соцработника кажется подозрительным – **до совершения любых действий посоветуйтесь с родственниками!**

- **Если вы сдаете квартиру без оформления договора – вы очень рискуете.** Бывали случаи переоформления квартир на жильцов, в т. ч. нелегалов. Тяжба по выселению последних может тянуться годами!

ЕСЛИ С ВАМИ СЛУЧИЛАСЬ БЕДА, ЗВОНИТЕ В ПОЛИЦИЮ! ВАМ ПОМОГУТ!

В СЛУЧАЕ ОСТРОЙ НЕОБХОДИМОСТИ

Добавьте в памятку необходимые вам номера, которых там не хватает: в экстренной ситуации вы легко и быстро найдете их.

Телефоны вызова экстренной помощи:

Служба спасения: с мобильного – **112** или **911**.

Полиция (центральный городской пульт): **02**

Ваш участковый: _____

Ваше отделение полиции
(срочный выезд патруля): _____

Скорая помощь: 03

При пожаре и задымлении: 01

Телефоны доверия УВД: _____

Диспетчерские аварийных служб (для проверки сотрудников):

Пожарная охрана (пожароопасная обстановка, визит инспектора): _____

Вызов службы газа,
проверка сотрудников: _____

Электросеть
(для вызова или проверки сотрудников): _____

РЭУ (ремонтная служба вашего дома): _____

Другие полезные телефоны:

Районная поликлиника (при визитах незнакомых медработников): _____

Патронажная служба (если к вам пришел незнакомый сотрудник): _____

Ветеранская организация (если вам предлагают льготы или просят ваши награды): _____

Ваши собственные данные (для врачей на случай болезни):

Ф. И. О.: _____

Адрес _____

_____

Информация о непереносимости лекарств:

_____

_____

Телефоны ближайших родственников:

_____

_____

_____

В последнее время наблюдается рост числа случаев мошенничества с пластиковыми картами. Управление «К» МВД РФ рекомендует всем владельцам пластиковых карт следовать правилам безопасности:

1. **НИКОМУ И НИКОГДА НЕ СООБЩАТЬ ПИН-КОД КАРТЫ**

2. **ВЫУЧИТЬ ПИН-КОД ЛИБО ХРАНИТЬ ЕГО ОТДЕЛЬНО ОТ КАРТЫ И НЕ В БУМАЖНИКЕ**

3. **НЕ ПЕРЕДАВАТЬ КАРТУ ДРУГИМ ЛИЦАМ – ВСЕ ОПЕРАЦИИ С КАРТОЙ ДОЛЖНЫ ПРОВОДИТЬСЯ НА ВАШИХ ГЛАЗАХ**

4. **ПОЛЬЗОВАТЬСЯ ТОЛЬКО БАНКОМАТАМИ НЕ ОБОРУДОВАННЫМИ ДОПОЛНИТЕЛЬНЫМИ УСТРОЙСТВАМИ**

5. **ПО ВСЕМ ВОПРОСАМ СОВЕТОВАТЬСЯ С БАНКОМ, ВЫДАВШИМ КАРТУ**

Сегодня банковские пластиковые карты постоянно используются в повседневной жизни. Они упрощают процесс оплаты, а главное – являются дополнительной защитой для денежных средств, ведь украденная карта бесполезна, если не знать ПИН-код.

Но безопасность средств, хранимых на банковском счете, зависит в первую очередь от того, соблюдает владелец правила пользования картой или нет. Небрежное обращение с картой работает на руку мошенникам, которые постоянно изыскивают новые способы обмана владельцев карт.

Проанализировав все случаи мошенничества такого рода, специалисты Управления «К» МВД России подготовили для Вас понятную и полезную памятку. Предлагаем внимательно ознакомиться с содержанием этой брошюры и следовать нашим рекомендациям. Они защитят Вас от действий мошенников и сберегут Ваши средства.

Министерство внутренних дел
Российской Федерации

Управление «К»
МВД РФ предупреждает!

ВЛАДЕЛЬЦАМ ПЛАСТИКОВЫХ БАНКОВСКИХ КАРТ

Будьте осторожны и внимательны!

Мошенничества
с пластиковыми картами

ПИН-КОД — КЛЮЧ К ВАШИМ ДЕНЬГАМ

Никогда и никому не сообщайте ПИН-код Вашей карты. Лучше всего его запомнить. Относитесь к ПИН-коду, как к ключу от сейфа с вашими средствами.

Нельзя хранить ПИН-код рядом с картой и тем более записывать ПИН-код на неё – в этом случае Вы даже не успеете обезопасить свой счёт, заблокировав карту после кражи или утери.

ВАША КАРТА – ТОЛЬКО ВАША

Не позволяйте никому использовать Вашу пластиковую карту – это всё равно что отдать свой кошелёк, не пересчитывая сумму в нём.

НИ У КОГО НЕТ ПРАВА ТРЕБОВАТЬ ВАШ ПИН-КОД

Если Вам позвонили из какой-либо организации, или Вы получили письмо по электронной почте (в том числе из банка) с просьбой сообщить реквизиты карты и ПИН-код под различными предлогами, не спешите её выполнять. Позвоните в указанную организацию и сообщите о данном факте. Не переходите по указанным в письме ссылкам, поскольку они могут вести на сайты-двойники.

Помните: хранение реквизитов и ПИН-кода в тайне – это Ваша ответственность и обязанность.

НЕМЕДЛЕННО БЛОКИРУЙТЕ КАРТУ В СЛУЧАЕ ЕЕ УТЕРИ

Если Вы утратили карту, срочно свяжитесь с банком, выдавшим её, сообщите о случившемся и следуйте инструкциям сотрудника банка. Для этого держите телефон банка в записной книжке или в списке контактов Вашего мобильного телефона.

ПОЛЬЗУЙТЕСЬ ЗАЩИЩЁННЫМИ БАНКОМАТАМИ

При проведении операций с картой пользуйтесь только теми банкоматами, которые расположены в безопасных местах и оборудованы системой видеонаблюдения и охраной: в государственных учреждениях, банках, крупных торговых центрах и т.д.

Использование банкоматов без видеонаблюдения опасно вероятностью нападения злоумышленников.

ОПАСАЙТЕСЬ ПОСТОРОННИХ

Совершая операции с пластиковой картой, следите, чтобы рядом не было посторонних людей. Если это невозможно, снимите деньги с карты позже либо воспользуйтесь другим банкоматом.

Реквизиты и любая прочая информация о том, сколько средств Вы сняли и какие цифры вводили в банкомат, могут быть использованы мошенниками.

БАНКОМАТ ДОЛЖЕН БЫТЬ «ЧИСТЫМ»

Обращайте внимание на картоприемник и клавиатуру банкомата. Если они оборудованы какими-либо дополнительными устройствами, то от использования данного банкомата лучше воздержаться и сообщить о своих подозрениях по указанному на нём телефону.

БАНКОМАТ ДОЛЖЕН БЫТЬ ПОЛНОСТЬЮ ИСПРАВНЫМ

В случае некорректной работы банкомата – если он долгое время находится в режиме ожидания или самопроизвольно перезагружается – откажитесь от его использования. Велика вероятность того, что он перепрограммирован мошенниками.

СОВЕТУЙТЕСЬ ТОЛЬКО С БАНКОМ

Никогда не прибегайте к помощи или советам третьих лиц при проведении операций с банковской картой. Свяжитесь с Вашим банком – он обязан предоставить консультацию по работе с картой.

НЕ ДОВЕРЯЙТЕ КАРТУ ОФИЦИАНТАМ И ПРОДАВЦАМ

В торговых точках, ресторанах и кафе все действия с Вашей пластиковой картой должны происходить в Вашем присутствии. В противном случае мошенники могут получить реквизиты Вашей карты при помощи специальных устройств и использовать их в дальнейшем для изготовления подделки.

Как распознать звонок мошенника

Обновлено 17.10.2022
Интернет и связь
Мошенничество
По данным МВД, за первое полугодие 2022 года телефонные мошенники похитили у россиян около 39 млрд ₽. Преступники постоянно придумывают новые способы обмана. Чтобы не попасться на их уловки, надо знать, как распознать мошенника и что делать при подобных звонках. Эти знания особенно важны для пожилых людей, поскольку именно они наиболее подвержены телефонному мошенничеству

Как стать киберграмотным в 60 лет
Как распознать мошенников

Звонят со скрытого номера
Звонки из банка идут с официальных номеров, указанных на сайте или на банковской карте. Вам могут позвонить из конкретного отделения банка, номер будет федеральным или мобильным, но не скрытым

Спрашивают данные карты
Мошенники спрашивают конфиденциальные данные вашей карты: коды для подтверждения платёжных операций, CVC/CVV — три цифры с обратной стороны банковской карты, логины и пароли, код-пароль из смс к личному кабинету на сайте банка или в мобильном приложении
Настоящий сотрудник банка никогда не спросит секретные реквизиты карты, ПИН-коды и пароли, а номер карты и срок её действия знает из системы обслуживания клиентов

Сообщают тревожную информацию
Мошенники нагнетают ситуацию, пытаясь вогнать жертву в панику, заставить действовать необдуманно, поспешно. В таком состоянии человек может поделиться с преступниками конфиденциальной информацией или перевести деньги на счёт обманщиков
Мошенники могут представиться сотрудниками банка и сообщить, что организация заблокировала счёт, начислила штраф за кредит или по карте проведена подозрительная операция. Представиться сотрудниками полиции, ФСБ, прокуратуры и запугать уголовным делом или сообщить о попавшем в беду родственнике. Под видом сотрудников Пенсионного фонда, Налоговой службы и даже Госуслуг запугивать отменой льгот, выплат и начислением штрафов

Давят на вас
Мошенники всегда торопят, чтобы не дать жертве времени обдумать ситуацию. Чаще всего звонят поздно вечером, ночью или ранним утром в выходные дни, когда человек спит и не может быстро сориентироваться. В ходе звонка предостерегают от самостоятельных попыток разобраться с проблемой

Сообщают о внезапном выигрыше

Мошенники сообщают о внезапном выигрыше в лотерею, предлагают прибыльную работу или беспроигрышные конкурсы. Взамен просят оплатить небольшой взнос — перевести на указанный счёт деньги или сообщить данные банковской карты

Уговаривают открыть ссылку из смс
Во время разговора мошенники сообщают, что вам пришла ссылка в смс, и настойчиво уговаривают её открыть. Так злоумышленники хотят, чтобы под видом антивируса или другой полезной программы вы установили вредоносную программу. Это позволит мошенникам получить доступ к вашему смартфону и похитить данные или деньги, воспользовавшись мобильным банком, или подписать на платные рассылки

Сбрасывают звонки
Мошенники звонят с неизвестного номера и сбрасывают звонок, чтобы вынудить жертву перезвонить на этот номер. Хитрость в том, что обратный звонок на подозрительный номер будет платным. Иногда мошенники оставляют сообщение в голосовой почте — это повышает шанс, что вы решите перезвонить
Как защитить себя от мошенников

Не паникуйте
Никогда не принимайте поспешных решений, особенно если они касаются ваших денег. Всегда берите паузу, чтобы разобраться в том, что происходит. Скажите, что перезвоните самостоятельно, и сразу завершите звонок. Иначе мошенники продолжат запугивать и давить на вас
Если возникли сомнения в безопасности банковских счетов, позвоните в банк по номеру с официального сайта или с пластиковой карты. Обязательно расскажите оператору о звонке мошенника и о том, что вы ему сообщили. При необходимости оператор заблокирует вашу карту или приостановит возможность проведения операций в интернет-банке
Не перезванивайте по номеру, с которого совершался звонок. Даже если он отображается как официальный номер организации, это может быть маскировка мошенников. Номер нужно набрать вручную

Не сообщайте логины и пароли от аккаунтов, платёжные данные, одноразовые коды из смс
Единственная ситуация, при которой требуется назвать устно одноразовый код, — личное обслуживание в банке или в магазине. Когда нужно подтвердить операцию, например выдачу банковской карты или списание бонусов программы лояльности

Установите программу или подключите сервис определения номеров мошенников у мобильного оператора или в банковском приложении
Эти сервисы распознают и блокируют звонки мошенников, в том числе замаскированные под официальные номера банков и ведомств. Номер проверяется в базе, и во время звонка высвечивается информация о том, кто вам звонит. Однако помните, что базы операторов не всегда обновляются автоматически, поэтому регулярно обновляйте их вручную и не теряйте бдительности

Не переводите деньги на счета, номера которых вам называют по телефону

Никакого «резервного счёта», который позволит спасти ваши деньги, не существует. Это счёт мошенников, и вы добровольно переведёте им свои деньги
Нельзя переводить деньги «сотруднику полиции», который обещает решить проблемы попавшего в неприятную ситуацию родственника. Даже если у ваших родных действительно возникли проблемы с законом, решать их нужно легальным путём

Не переходите по ссылкам, которые присылают во время звонка
Не устанавливайте навязываемые приложения: никаких «специальных антивирусов» не существует. Всю необходимую информацию можно найти на официальных сайтах банков, а безопасные программы ищите в магазинах приложений — у них строгая модерация, рейтинг, статистика по количеству скачиваний и отзывы пользователей
Резюме

- Не паникуйте. Просто скажите «я вам перезвоню» и завершите разговор
- Ни под каким предлогом не называйте личные данные, реквизиты карты и секретную информацию: CVC/CVV-код на обратной стороне карты, коды из смс и ПИН-коды
- Не переводите деньги на счета незнакомых вам людей
- Не устанавливайте на смартфон приложения из непонятных источников
- Всегда набирайте официальный номер банка. Он указан на официальном сайте или на обратной стороне карты. Расскажите оператору о проблеме
- Любые вопросы решайте в рамках закона
- Установите программу, которая проверяет звонки и умеет блокировать спам-вызовы

Как не стать жертвой фишинга

Обновлено 17.10.2022
Интернет и связь
Мошенничество
Фишинг — вид интернет-мошенничества, цель которого получить доступ к секретным данным пользователя: логинам и паролям, номерам карт, банковским счетам. Преступники присылают фишинговые письма, которые могут быть очень похожи на настоящие сообщения от банков, компаний, органов власти или Госуслуг. Но ссылка в таком письме ведёт на поддельный сайт. Став жертвой фишинга, можно лишиться денег или доступа к своим аккаунтам, пустить хакера в корпоративную сеть работодателя. Фишинговыми бывают не только письма, приходящие на электронную почту. Это могут быть сообщения в мессенджерах, социальных сетях и смс. Рассказываем, как распознать и защититься от фишинга
Примеры фишинга

Сообщение о выигрыше или назначенной выплате от государства
При переходе по ссылке откроется фейковый сайт, на котором вам предложат ввести данные банковской карты для получения выигрыша. Так мошенники получат доступ к вашей карте и могут списать с неё все деньги. Иногда сайты, на которые ведёт ссылка из сообщения, заражены вирусами и пытаются загрузить на ваше устройство вредоносные программы

Сообщение о необходимости смены пароля
Злоумышленники имитируют письма от администрации социальных сетей, интернет-магазинов. В письмах просят пользователя сменить пароль. При переходе по ссылке вы окажетесь на сайте, который оформлен как настоящий интернет-сервис. На странице предложат ввести старый пароль и придумать новый. Так действующий пароль от вашего аккаунта окажется у мошенников

Письмо с выгодным предложением
Киберпреступники рассылают письма от имени интернет-магазинов, сервисов доставки еды и брокерских контор. Ссылки из таких писем ведут на поддельные сайты, которые похожи на настоящие. Цель преступников — заставить вас поверить, что это реальный магазин, сервис, брокер, чтобы вы совершили покупку онлайн. Никаких товаров и услуг вы не получите, а мошенники скроются с вашими деньгами

Письмо от отдела кадров, ИТ-департамента, партнёров или подрядчиков
Мошенники имитируют письма от ваших коллег, клиентов или подрядчиков. Письмо может содержать ссылку на фишинговый сайт или вложение с вредоносной программой. Цель хакеров — получить доступ к вашей рабочей учётной записи или заразить вирусом корпоративный компьютер. Это может стать началом кибератаки на вашего работодателя

Поддельные приложения
Мошенники используют в своих схемах приложения для смартфонов, планшетов и компьютеров. Эти программы содержат вирусы, которые крадут банковские реквизиты, логины и пароли от мобильного или онлайн-банка, а также перехватывают смс с кодами. Чаще подделывают мобильные банки — если ввести логин и пароль, хакеры получат доступ к вашим счетам в настоящем приложении

Как защититься от фишинга

Внимательно проверяйте адрес отправителя
Адрес сайта (URL) может отличаться от настоящего всего одной буквой, символом или доменом. Проанализируйте адрес сайта, на который были переадресованы, например он может заканчиваться на .com вместо .gov. или иметь вид https://www.gossuslugi.ru/ вместо https://www.gosuslugi.ru/ с двойной «s»

Не переходите по подозрительным ссылкам в сообщениях
Получив сообщение на почту, в соцсети, мессенджер, не переходите по ссылкам из писем, если вы их не запрашивали. Уведомление из банка или от онлайн-магазина можно проверить, позвонив по телефону с официального сайта
С подозрением относитесь к рекламным баннерам на сайтах — они могут вести на фишинговый сайт или содержать в себе вредоносный код

Проверяйте информацию из рассылок
Если в письме пришло приглашение принять участие в акции компании, проверьте информацию на её официальном сайте, который найдёте через поисковик. Это касается и ситуации, когда вам сообщают о новых выплатах — всю информацию о них можно найти на Госуслугах или официальных сайтах органов власти

Меняйте пароли в самом сервисе
Не переходите по ссылкам о смене пароля или других учётных записей, чтобы поменять их. При необходимости меняйте пароли через личный кабинет, а не по ссылке из соответствующего письма. Не путайте смену пароля с ситуацией восстановления пароля, когда вы сами запрашиваете ссылку, которая придёт в письме

Скачивайте программы из официальных магазинов приложений
Обращайте внимание на количество скачиваний, рейтинг и отзывы. Если программа совсем новая и её пока мало кто установил, лучше не рисковать. Смотрите отзывы не только в магазине приложений, но и на профильных форумах. Так вы узнаете, не возникало ли проблем с программой в последнее время
Если необходимо установить приложения банков, попавших под санкции, скачайте их с официальных сайтов организаций

Сообщайте о подозрительных письмах на рабочей почте службе безопасности или ИТ-отделу

Прежде чем перейти по ссылке из такого письма или открыть вложение, созвонитесь с отправителем и узнайте, действительно ли это письмо от него

Повышайте киберграмотность
Проверяйте свои знания, чтобы понять, насколько хорошо вы умеете распознавать фишинг. С этим помогут тесты по кибербезопасности. При необходимости пройдите курсы цифровой безопасности, иногда такое обучение устраивает работодатель

Как защитить мобильное устройство

Обновлено 17.10.2022
Интернет и связь
Мошенничество
Киберпреступники постоянно охотятся за чужими личными данными. Часто их целью является секретная информация из смартфонов: номера карт, доступы к онлайн-банкам, домашний адрес, рабочие документы и личные фото. Рассказываем, как защитить свой телефон от действий злоумышленников

Какие бывают угрозы

Случайный доступ

При использовании одного устройства несколькими членами семьи следует контролировать доступ к конфиденциальной информации. Не разрешайте ребёнку использовать устройство, на котором хранится важная информация, а также установлены приложения мобильного банка, почты и другие

Кража

Если у вас украли смартфон, потери могут не ограничиться самим телефоном. Вор может получить доступ к вашим аккаунтам, которые привязаны к устройству. Воспользоваться мобильным банком и вывести с ваших счетов все доступные деньги. Использовать для шантажа и вымогательства вашу личную информацию — рабочие документы, фото, переписки в мессенджерах и соцсетях

Действия хакеров

Киберпреступники атакуют смартфоны с помощью вредоносных программ или файлов с вирусами, получают удалённый доступ к гаджетам и крадут с них секретные данные. Такая ситуация опаснее реальной кражи устройства — человек может не подозревать, что его информацию похитили

Как защитить устройство на случай кражи

Настройте блокировку экрана

Для защиты устройства включите автоматическую блокировку экрана. Для разблокировки используйте длинные пароли и сканер отпечатка пальца. Графический ключ легко подглядеть из-за плеча и несложно подобрать — люди рисуют слишком очевидные траектории

Защитите паролем или отпечатком пальца важные приложения и файлы

Это станет дополнительным фактором защиты и не позволит вору быстро попасть в банковские приложения, диспетчер файлов, галерею, почту, ваши аккаунты в социальных сетях

Как создать надёжный пароль, который легко запомнить

Настройте отслеживание

Установите программу, которая удалённо блокирует телефон. Такие приложения определяют местоположение устройства, включают сирену, фотографируют злоумышленника, а также стирают все личные данные

На мобильных устройствах по умолчанию установлена функция «Найти устройство», которая позволяет также удалённо заблокировать смартфон и удалить с него все данные. Убедитесь, что функция не отключена. Чтобы не потерять свои данные, регулярно делайте резервные копии. Важно, чтобы эти копии хранились в недоступном для злоумышленников месте, например на съёмном диске

Как защититься от киберпреступников

Скачивайте только проверенные приложения

Злоумышленники распространяют вредоносные программы под видом игр и полезных приложений. Загружайте приложения только из официальных магазинов: здесь строгая модерация, рейтинг, статистика по количеству скачиваний и отзывы пользователей

Если необходимо установить приложения банков, попавших под санкции, скачайте их с официальных сайтов организаций

Не переходите по подозрительным ссылкам

Чтобы заразить телефон вирусом, злоумышленники часто рассылают письма и сообщения с информацией о выигрыше, выгодной акции. При переходе по ссылке из такого сообщения на смартфон может загрузиться вредоносная программа. Если случайно перешли и файл загрузился, ни в коем случае не открывайте его и удалите

Установите антивирус на смартфон

Антивирусы смогут обнаружить вредоносную программу, если она уже оказалась на устройстве. Защитные системы блокируют переходы на заражённые сайты, проверяют ссылки, которые приходят в смс и мессенджерах, выявляют небезопасные настройки на смартфоне. Не забывайте периодически обновлять антивирус

Не давайте приложениям лишних разрешений

Не разрешайте приложениям, например планировщику дел или фонарику, получать доступ к камере, файлам на устройстве, совершению звонков, отправке смс.

Если приложение получает подобные разрешения, оно сможет пользоваться этими функциями без вашего ведома — отправлять ваши фотографии на сервер злоумышленников или подписывать на платные рассылки. Разрешения приложений можно проверить в общих настройках телефона

Постоянно обновляйте систему

Киберпреступники ищут уязвимости в программном обеспечении и приложениях, поэтому разработчики программ регулярно выпускают обновления, исправляют ошибки и уязвимости. Включите автоматические обновления операционной системы в установленных приложениях. Если обновления не устанавливать, устройство будет хуже защищено от новых киберугроз

По возможности откажитесь от бесплатного вайфая

Публичные сети могут быть недостаточно защищёнными. Злоумышленники взламывают и перехватывают трафик, который идёт с вашего устройства. В их руках окажутся секретные данные, в том числе логины и пароли от различных аккаунтов. Кроме того, мошенники могут сами размещать точки доступа и выдавать их за бесплатный вайфай в парках, кафе и торговых центрах