Банк России

БЕЗОПАСНОСТЬ МОБИЛЬНЫХ УСТРОЙСТВ

Почему важно знать правила безопасной работы со смартфоном?

- Смартфон - это не просто средство связи или красивая игрушка, но и цифровая копия всей жизни пользователя

- Для злоумышленника смартфон любого человека - неиссякаемый источник информации и денег, а также множество способов получить доступ к личным аккаунтам «жертвы»

Что может сделать злоумышленник?

- копировать и удалять вашу информацию
- показывать рекламу
- устанавливать приложения
- отправлять сообщения и т.д.
- украсть деньги
- получить доступ к рабочей переписке
- получить данные, с помощью которых можно нанести ущерб вашей организации – организовать кибератаку

Защита физического доступа

- **Используйте автоматическую блокировку экрана.** Оптимальное время автоматической блокировки: 1,5 - 2 минуты бездействия
- Отключите предпросмотр сообщений при выключенном экране
- Будьте осторожны с функцией голосового помощника: она должна быть отключена при заблокированном экране

Как защитить смартфон?

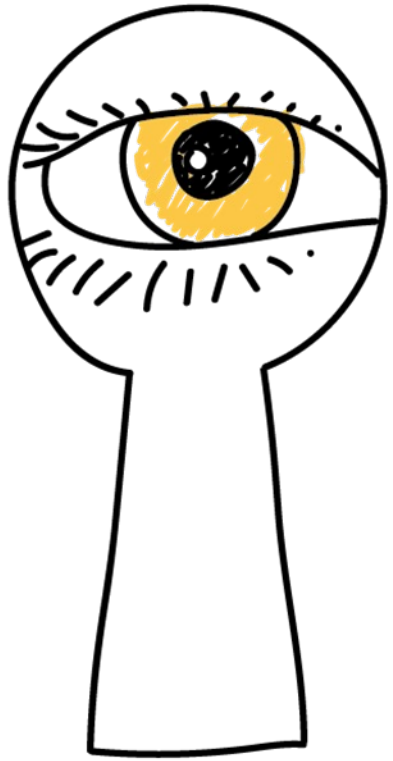
- Настройте функцию удаленного управления устройством в случае потери или кражи
- Регулярно делайте резервные копии
- Обязательно блокируйте доступ к устройству надежным паролем
- Перепишите себе IMEI и серийный номер устройства
- При потере рабочей информации сразу сообщите ответственным за безопасность

Украли или потеряли телефон. Что делать?

- Зайдите в программу удаленного администрирования мобильного устройства и заблокировать его. Выведите на экран свои контактные данные
- Включите отслеживание телефона
- Позвоните на смартфон или воспользуйтесь функцией «Прозвон»
- Удаленно сотрите все данные
- Свяжитесь с сотовым оператором и заблокируйте SIM-карту
- Свяжитесь с банковскими сервисами и сообщите, что смартфон украли и привязка к счетам недействительна
- Обратитесь в органы правопорядка

Защита от вредоносного ПО

- Необходимо защищать мобильные устройства от вредоносного ПО
- Мобильное вредоносное ПО пытается получить доступ к банковским данным, логину/паролю, заблокировать телефон, шпионить за вами и т.д.
- Если смартфон заражен вредоносным ПО – крайне важно выявить это как можно скорее



Как понять, что на смартфоне есть вредоносное ПО?

- смартфон быстро разряжается, нагревается и «тормозит»
- экраны известных приложений выглядят необычно
- появляются неожиданные всплывающие окна и показывается слишком много рекламы
- появляются запросы на установку неизвестных приложений
- приложения не принимают ваши пароли
- неизвестные приложения запрашивают доступ к СМС, контактам, звонкам, геолокации и т.д.
- быстро кончаются деньги на мобильном счете и многое другое

Что делать?

- Просканируйте устройство антивирусом
- Постарайтесь воздержаться от использования смартфона
- Если вы авторизовывались на каких-либо сервисах, зайдите на них с другого устройства и поменяйте все пароли
- Покажите устройство специалисту. Если проблемы с вашим личным устройством, отнесите его в фирменный или авторизованный центр обслуживания компании-производителя устройства

Если вы проигнорируете признаки заражения – последствия могут быть самыми неприятными

Как попадает вредоносное ПО?

Вредоносное ПО может попасть на смартфон:

- из «неофициального» магазина приложений
- из бесплатных «пиратских» программ
- в результате обмана злоумышленниками (классический «фишинг», вредоносные ссылки и сайты)

Как избежать вредоносного ПО?

ВСЕГДА

- устанавливайте приложения только из официальных магазинов

НИКОГДА

- не устанавливайте пиратское и нелицензионное ПО
- не переходите по подозрительным ссылкам, не посещайте пиратские сайты, не загружайте неизвестные файлы из Интернета

Как избежать вредоносного ПО?

- Чтобы не попасться на «фишинговую» ссылку, всегда смотрите ее реальный адрес. Для этого:
  - зажмите и удерживайте ссылку нажатой
  - в выпавшем меню выберите «скопировать ссылку»
  - вставьте скопированное в записную книжку
- Если скопированный адрес не совпадает с тем, что рекламирует название ссылки – по ней лучше не переходить

Например, ссылка «лучший рецепт яблочного пирога» не должна вести на https://malwareevil.com/downloads/supervirus.exe

Как безопасно устанавливать приложения?

- обращайте внимание на опечатки в названиях (например tellegram вместо telegram)
- смотрите на количество скачиваний
- обращайте внимание на рейтинг
- читайте отзывы и обращайте внимание на их качество (живые люди пишут отзывы по-разному: иногда с ошибками, иногда нецензурно, иногда нелогично)
- посмотрите сторонние рейтинги

По возможности скачивайте приложения по ссылкам с официальных сайтов разработчиков

Использование бесплатного WI-FI

ЧТО НУЖНО СДЕЛАТЬ

- отключить функцию автоподключения к открытым Wi-Fi сетям
- использовать только защищённые Wi-Fi сети (безопасное соединение, которое обозначено замком с зелёным текстом и режим «приватного просмотра» в браузере)
- обязательно правильно завершать работу с публичным Wi-Fi (всегда используйте кнопку «выйти»)
- при работе с публичным устройством используйте пункт «чужой компьютер» и отказывайтесь от сохранения пароля

Безопасно ли подключать смартфоны к компьютерам?

Правила

- не используйте смартфон в качестве USB-носителя
- не заряжайте смартфон от компьютеров и общественных точек зарядки – используйте внешний аккумулятор

Почему нельзя заряжать смартфон от общественного USB-порта?

Существует отдельный тип кибератак на смартфоны – это juice jacking, или **«соковыжималка»**

Подключаете смартфон в режиме зарядки, передача данных по умолчанию отключена. Но те контакты USB-соединения, которые отвечают за передачу данных, никуда не делись, и если злоумышленник имеет доступ к стороне, с которой поступает электроэнергия, он может точно так же передавать на ваш смартфон информацию или получать ее

Подключение по Bluetooth

Правила

- Никогда не подключайтесь по Bluetooth к незнакомым устройствам

- При отсутствии необходимости держите Bluetooth отключенным

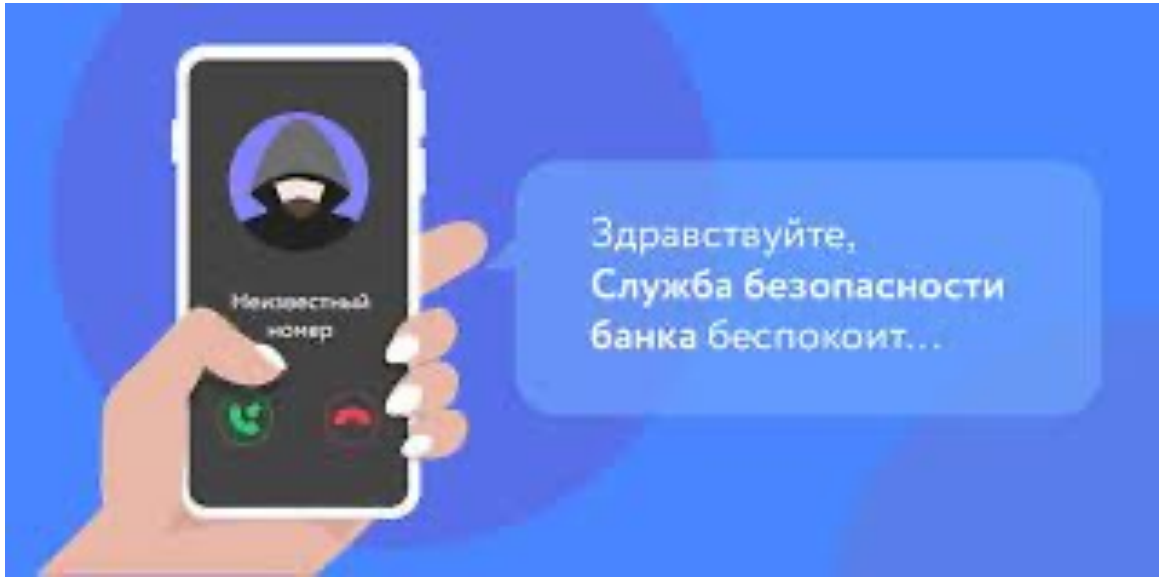
Как безопасно пользоваться соцсетями?

ПРАВИЛА БЕЗОПАСНОСТИ

- При регистрации в социальных сетях информацию о себе вводите осознанно
- Настройте приватность в соц. сетях и других сервисах
- Не публикуйте информацию о своём местонахождении и (или) материальных ценностях
- Хорошо подумайте, какую информацию можно публиковать в Интернете
- Не доверяйте свои секреты незнакомцам из Интернета
- Ведите себя в Интернете вежливо, как в реальной жизни

Телефонный фишинг

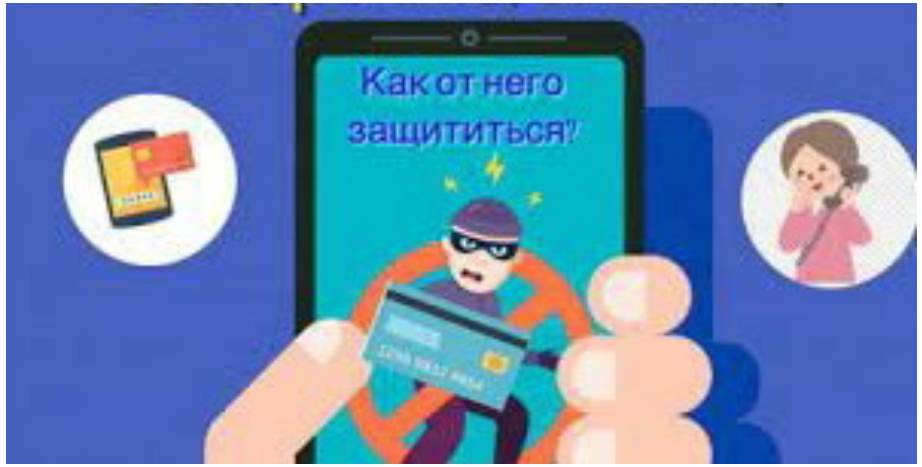
- Подмена номера
- Банковская многоходовка
- С вашим родственником случилось несчастье
- Установите приложение
- Перепутанный счет
- Возмещение ущерба
- Сброс звонка



Телефонный фишинг

Правила

- Никогда не сообщайте никаких данных незнакомым людям, позвонившим вам по телефону
- Никогда не переводите никаких средств по рекомендации или просьбе незнакомых людей, позвонивших вам по телефону
- Не торопитесь с выводами



Спасибо за внимание!

И не попадайтесь на уловки мошенников!