Информация – очень ценный ресурс, и ее нужно уметь надежно защищать.

По данным Минцифры за 2023 год, больше половины всех утечек происходит по вине сотрудников. Даже утечка по незнанию может повлечь штрафы и санкции

Кибербезопасность (информационная безопасность)

Что это?

Из Указа Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»:
Информационная безопасность – состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства

Почему это важно?

Знание кибербезопасности помогает:

- Защищать конфиденциальные данные
- Распознавать атаки методом социальной инженерии и защищаться от них
- Формировать устойчивую культуру безопасности компании
- Обнаруживать и предотвращать внутренние и внешние угрозы
- Уменьшать количество ошибок по незнанию
- Повышать рейтинг компании

Киберпреступность

Что это?

Киберпреступность – любое преступление, совершаемое электронным способом.
Может включать в себя:

- Кражи
- Мошенничество
- Манипуляции

Почему это важно?

- Преступность представляет опасность как в реальной жизни, так и в сети
- Основы кибербезопасности могут во многом помочь уберечь ваши данные от попадания в руки злоумышленникам

Примеры киберпреступлений

- Кража личных данных
- Финансовая кража
- Кража и продажа корпоративных данных
- Кибершантаж (требование денег для предотвращения кибератаки)
- Атаки на сотрудников и компанию (фишинг, смишинг, вишинг, программы-вымогатели, атаки грубой силой, услуга за услугу)

Виды информации

Информация ограниченного доступа

Государственная тайна

Конфиденциальная информация

Общедоступная информация

Информация, доступ к которой не может быть ограничен

Иная информация

Типы конфиденциальной информации

Персональные данные

Ф. И. О., адреса, телефоны, паспортные данные, медицинские сведения

Коммерческая тайна

Патенты, изобретения, технологии, рецепты, алгоритмы

Служебная тайна

Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами

Сведения, связанные с профессиональной деятельностью

Врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений

Сведения о сущности изобретения

Сведения полезной модели или промышленного образца до официальной публикации информации о них

Тайна следствия и судопроизводства

Сведения, составляющие тайну следствия и судопроизводства, сведения о защищаемых лицах и мерах государственной защиты, осуществляемой в соответствии с нормативноправовыми актами Российской Федерации

Законодательство в области кибербезопасности

За нарушение законов в сфере кибербезопасности могут грозить серьезные последствия

Для сотрудника:

- Дисциплинарная ответственность
- Гражданско-правовая ответственность
- Административная ответственность
- Уголовная ответственность
- Штраф
- Увольнение

Для организации

- Юридическая ответственность
- Штраф
- Компенсация
- Ущерб репутации
- Нарушение заключенных договоров

Потенциально опасные действия

Вы случайно отправили электронное письмо тезке целевого получателя в другую компанию
Всегда проверяйте получателя дважды при отправке письма

Вы узнали от контрагента, что из-за хакерской атаки информация о партнерах была скомпрометирована. Но вы не сообщили об инциденте специалистам по ИТ
Немедленно сообщайте о любых инцидентах в ИТ-отдел

Вы потеряли пропуск от входа в офис и никому не сообщили об этом (или сообщили несвоевременно)
Оберегайте пропуск и не передавайте его никому. В случае потери сразу сообщите об этом в ИТ-отдел

Вы пропустили курьера, который сказал, что приехал отдать документы
Никогда не пропускайте посторонних лиц. Отводите курьеров и посетителей к охране или стойке регистрации

Вы опубликовали на профессиональном форуме данные об устройстве рабочих систем. Хакеры сохранили ваши данные и продают их в даркнете
Будьте внимательны к той информации, которую собираетесь публиковать. Если вы узнали, что данные утекли, сразу же сообщите об этом в ИТ-отдел

Вы скопировали конфиденциальные документы в личное облачное хранилище, которое взломали злоумышленники
Не копируйте никакие рабочие данные на личные устройства или в личное облачное хранилище

Вы оставили свой компьютер разблокированным и ушли на обед
Всегда блокируйте все устройства перед тем, как покинуть рабочее место

Что требуется от вас

Знать, что угрожает организации

Знать правила безопасности

Работать, соблюдая эти правила

Выполнение этих требований поможет защитить организацию, компьютерные системы и данные граждан (клиентов)

Связь с ИТ-отделом

Чтобы предотвратить распространение атаки по всем сотрудникам, сообщайте в ИТ-отдел все, что кажется вам подозрительным. Чем быстрее удастся предупредить об этом всех, тем меньше шансов на успех у злоумышленников

Ваши наблюдения – ценный источник знаний для ИТ-отдела

Чем выше уровень осведомленности сотрудника о базовых правилах кибербезопасности, тем меньше вероятность реализации атаки

Обратитесь в ИТ-отдел, если

1. Получили подозрительное письмо
2. Ввели данные на подозрительном сайте или просто посетили такой сайт
3. Заметили подозрительную активность на своем компьютере
4. Совершили ошибку, которая могла привести к раскрытию конфиденциальной информации
5. Нашли флешку или другое неизвестное оборудование
6. Заметили любые иные угрозы, связанные с кибербезопасностью
7. У вас есть вопросы, связанные с защитой информации

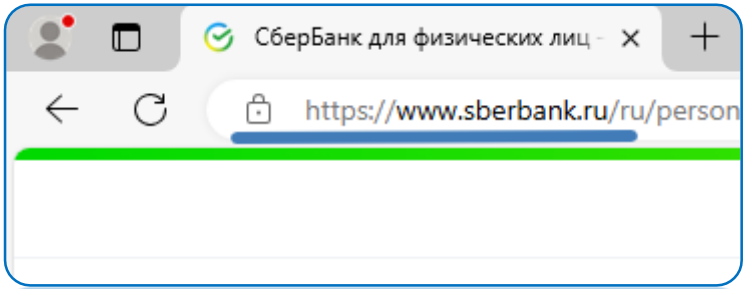
Работа с интернетом

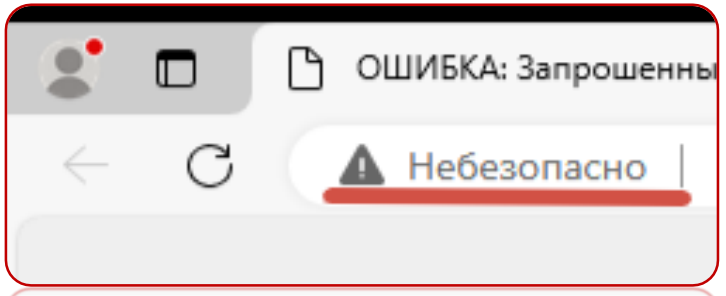
Кибербезопасность организации –основа её успеха

Умение сотрудника правильно работать в интернете, вовремя сообщать об атаках и знать, как предотвратить воздействие мошенников, поможет защитить организацию

1. Проверяйте адресную строку

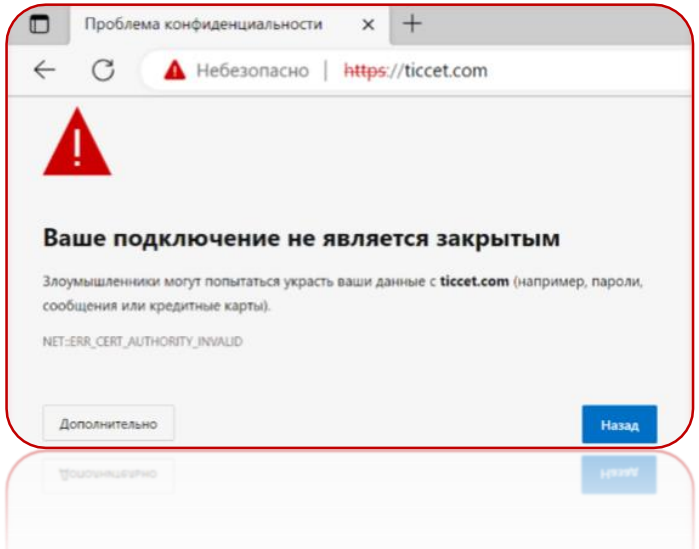
- Если вы собираетесь вводить на сайте важную информацию, проверьте его адрес в адресной строке браузера
- Все приемы с подделкой адреса рассчитаны на невнимательность и спешку пользователя
- Адрес сайта отображается в строке браузера, когда вы туда заходите
- Будьте осторожны: внешний вид ссылки и то, куда она в действительности ведет, могут не совпадать





2. Обращайте внимание на оповещения антивирусной программы и браузера

Если антивирус, установленный на вашем устройстве, предупреждает и предлагает выбрать, переходить или нет, это повод насторожиться и не переходить на сайт. Попробуйте найти нужный вам сайт повторно или поищите необходимую информацию на других ресурсах



3. Проверяйте страницу на наличие грамматических, орфографических и дизайнерских ошибок

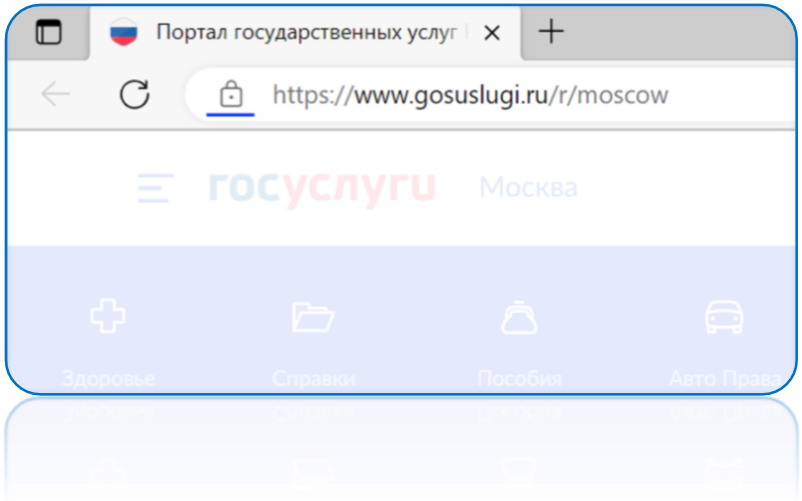
Довольно часто распознать мошенников можно по наличию грамматических и орфографических ошибок в тексте страниц. Крупные компании имеют в штате или на аутсорсинге профессиональных дизайнеров, копирайтеров, редакторов и корректоров, которые строго следят за соблюдением правил оформления сайта

Насторожить должны

- неправильное название организации
- обилие опечаток и ошибок
- поехавшая верстка
- неправильное использование цветов в дизайне
- наличие посторонних элементов дизайна

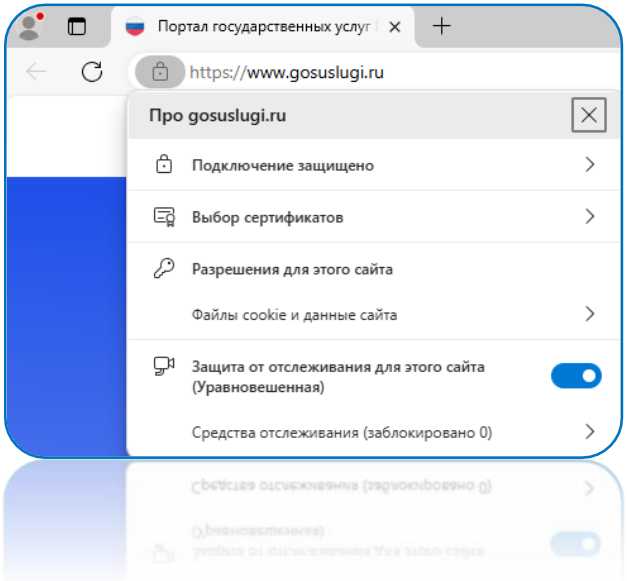
4. Проверяйте наличие SSL-сертификата

Если в строке перед адресом есть значок замочка, а перед именем сайта указан протокол HTTPS, значит, сайт имеет SSL-сертификат, а соединение между сервером и браузером пользователя зашифровано и безопасно



Проверяйте наличие SSL-сертификата

Кликнув на замочек, можно узнать больше о владельце сертификата. Нажмите на кнопки «Подключение защищено» и «Показать сертификат», чтобы увидеть название организации, которой принадлежит сайт

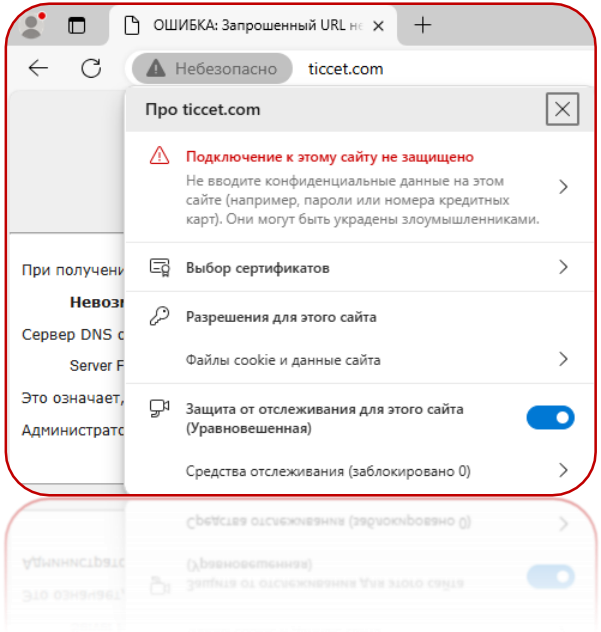


Проверяйте наличие SSL-сертификата

Если в строке перед адресом – восклицательный знак в треугольнике и предупреждение о том, что соединение не защищено, значит, у сайта нет SSL-сертификата.

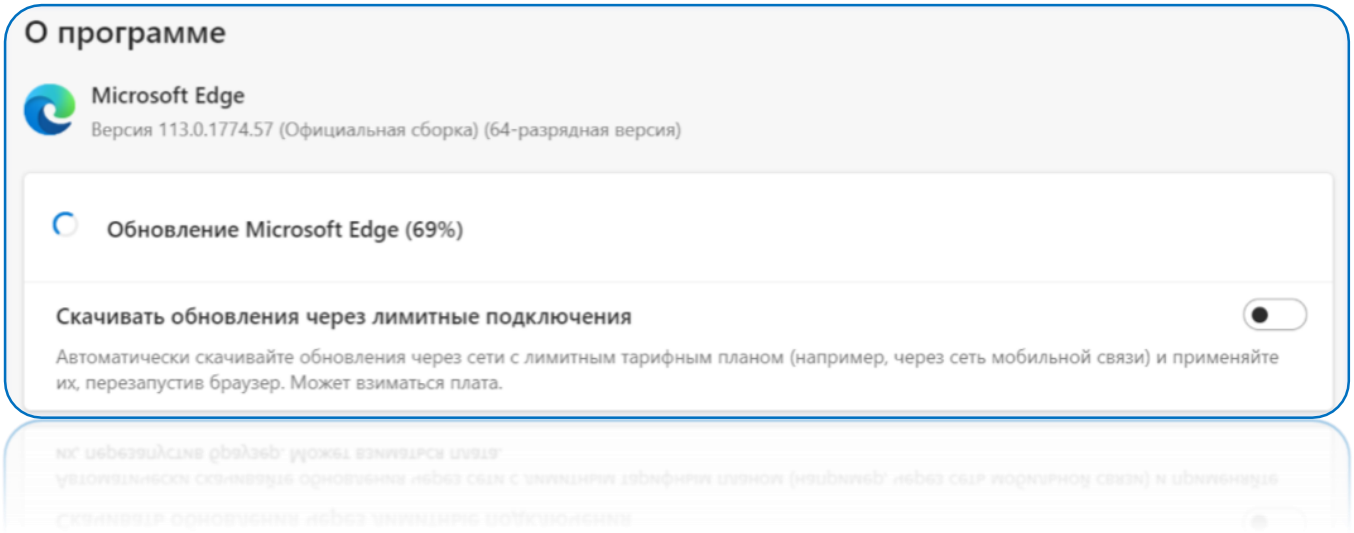
Это означает, что сайт использует протокол HTTP (ряд браузеров отображает его в адресной строке).
На таком сайте небезопасно вводить данные.

Сайты без SSL-сертификата передают и принимают данные в открытом виде, поэтому их легче перехватить и подменить



5. Обновляйте систему и все программы

Чтобы обеспечить безопасность в интернете, обновляйте браузер. Новые версии браузеров содержат исправления уязвимостей, которые могут быть использованы злоумышленниками либо вредоносным программным обеспечением для взлома ваших учетных данных или установки вредоносных программ



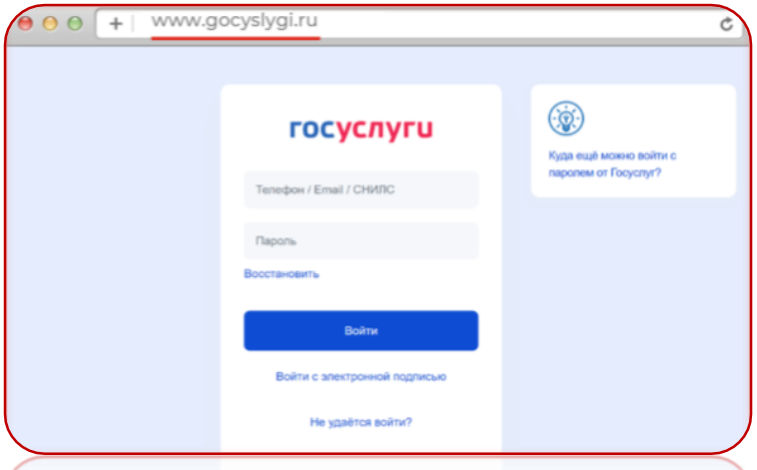
6. Изучите, какие сайты могут содержать поддельную форму ввода данных

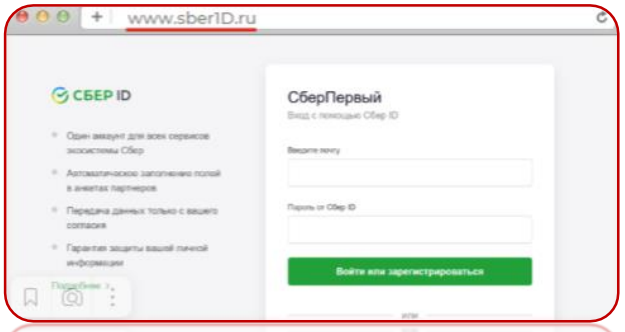
Чтобы пользователи вводили на сайтах свои данные, мошенники правдоподобно подделывают эти сайты

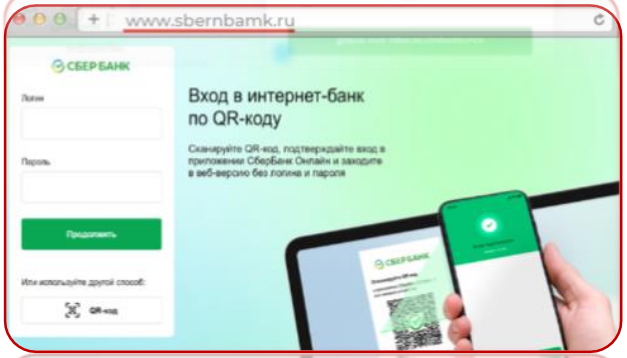
Внимательно изучите сайт, прежде чем вводить на нем свои данные, и не переходите по подозрительным ссылкам!

Примеры фишинговых сайтов

Фишинговый сайт – это мошеннический поддельный сайт, который внешне не отличается от оригинала. Выдает клона только его адресная строка



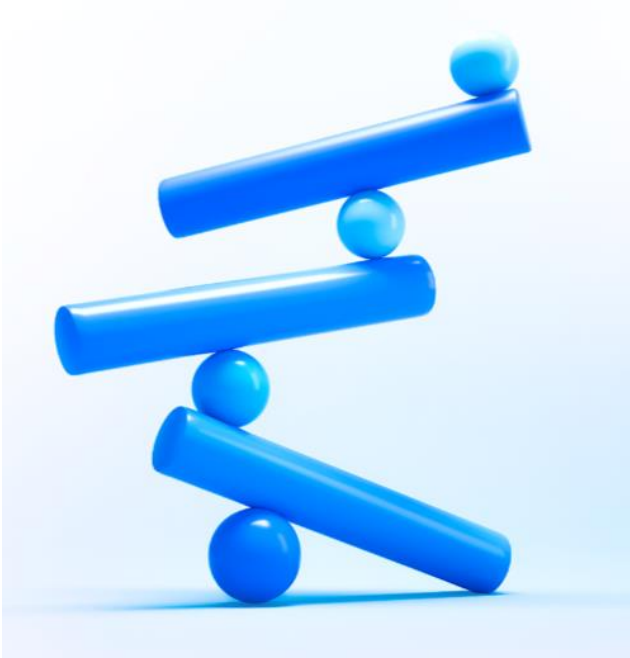




7. Используйте сложные пароли

Чем длиннее пароль,
тем сложнее его взломать

Для запоминания сложных
паролей используйте
менеджер паролей или
собственную память



8. Сохраняйте сайты в избранном

Для безопасности и экономии времени сохраняйте доверенные сайты, с которыми вы постоянно работаете, в закладки браузера и открывайте их оттуда

9. Выходите из всех аккаунтов

По возможности не заходите в свои учетные записи с чужих устройств. Если это все же необходимо, по завершении работы разлогиньтесь и закройте соответствующие вкладки

10. Подключите двухфакторную аутентификацию

Тогда для входа в аккаунт помимо пароля у вас запросят дополнительную информацию, например цифровой код, который отправляется по СМС/email или вычисляется через специальное приложение-аутентификатор на смартфоне

Запомните правила безопасной работы

Если после перехода на сайт у вас запрашивают какую-то личную информацию (Ф. И. О., email) или просят что-то скачать, не делайте этого

www

Проверяйте адрес сайта, если собираетесь вводить на нем важные данные: точно ли это тот сайт, который вам нужен

Не заходите с рабочего компьютера на сайты, не связанные с рабочими задачами

Пользуйтесь мобильным интернетом, а не публичным Wi-Fi, если вам необходимо что-то скачать или ввести данные на сайте вне дома/офиса

Выходите из своих учетных записей, если не работаете там в текущий момент

Сохраняйте сайты, на которых вы часто работаете, в закладки и заходите на них оттуда

Работа с электронной почтой

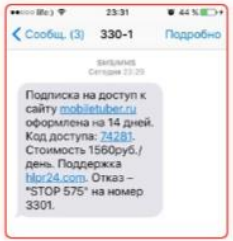
Электронная почта может быть источником угроз кибербезопасности для организации

Хакеры постоянно добывают и перепродают друг другу базы клиентов и сотрудников компаний. Получив список сотрудников с адресами, преступники могут атаковать организацию, рассылая серию вредоносных электронных писем, поэтому необходимо знать простые правила безопасности при работе с электронной почтой

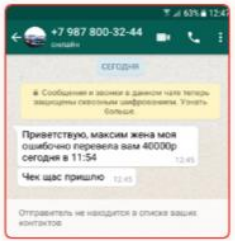
Фишинг

Фишинг (от англ, phishing) – способ получить личные данные пользователей обманным путем. На сегодняшний день это самый простой и эффективный способ взлома системы защиты организации в целом или компьютера конкретного человека

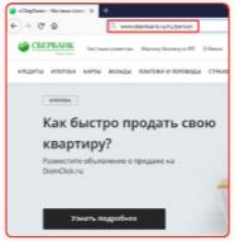
Разновидности фишинга



Мошеннические СМС (смишинг)



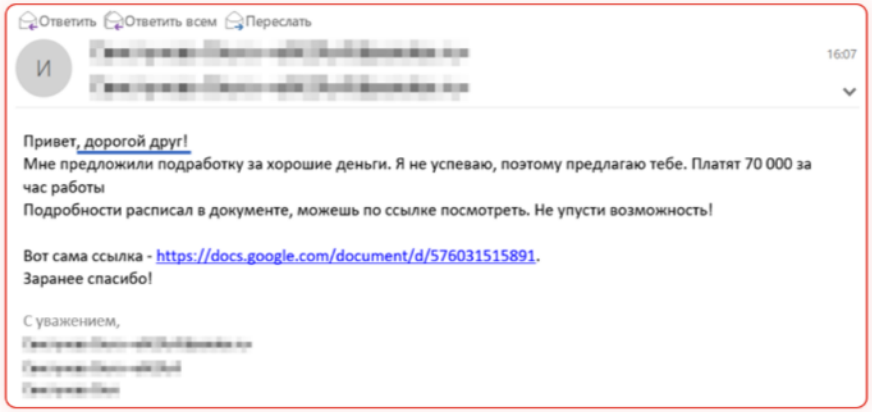
Сообщения в мессенджерах или социальных сетях

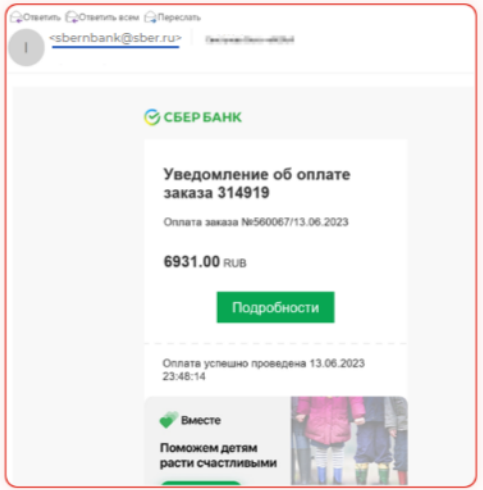


Поддельные сайты и реклама в интернете

Сообщения по электронной почте

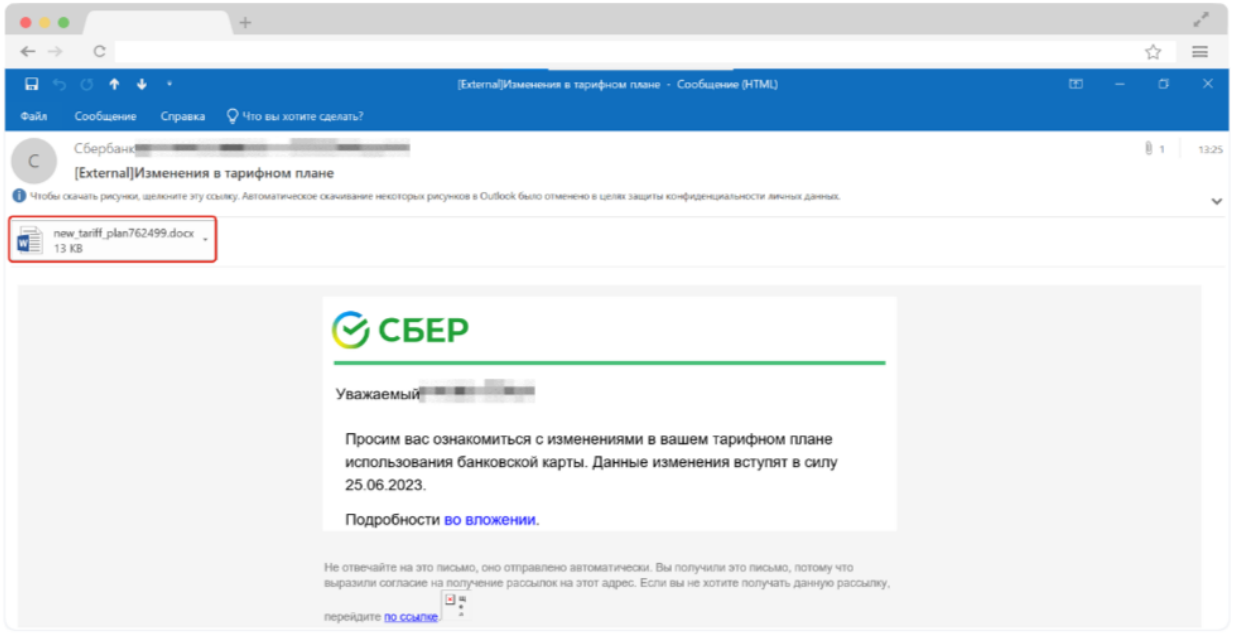
Примеры фишинговых атак





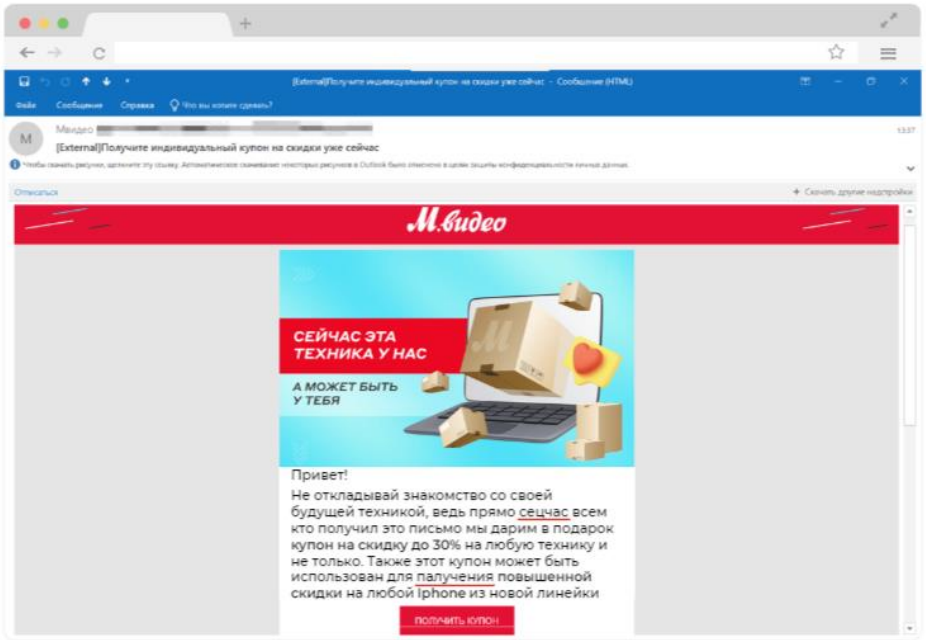
Как распознать фишинговое письмо

Письмо содержит подозрительные ссылки в тексте
либо документы и другие файлы в приложении



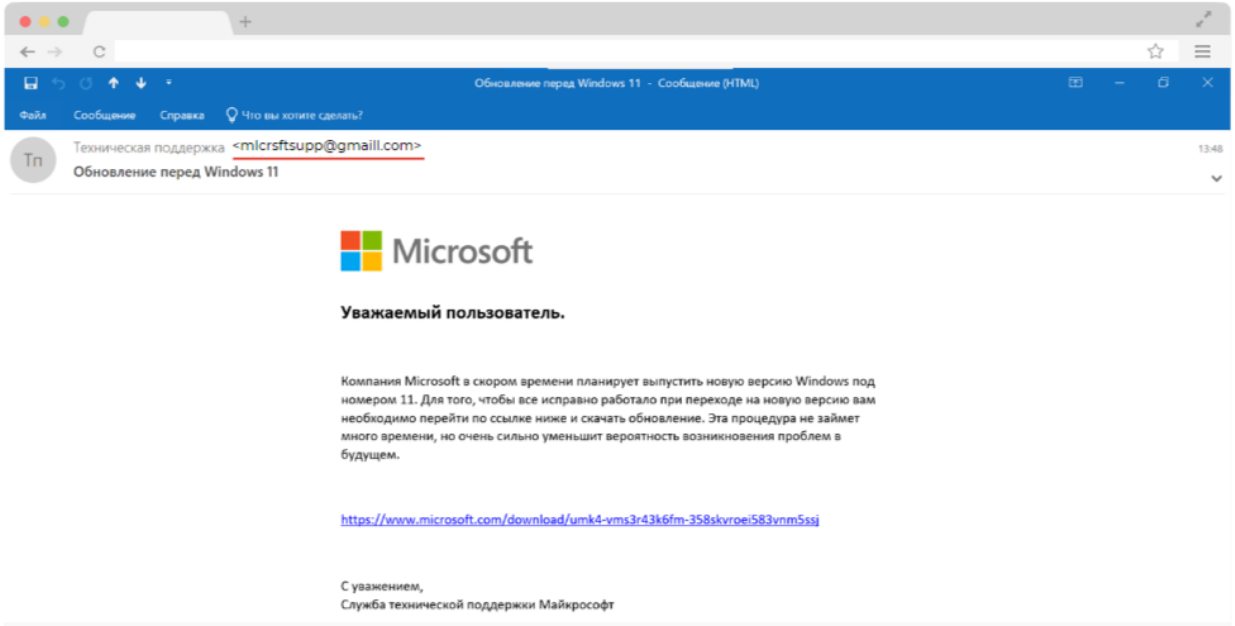
Как распознать фишинговое письмо

Письмо содержит грубые ошибки и/или опечатки



Как распознать фишинговое письмо

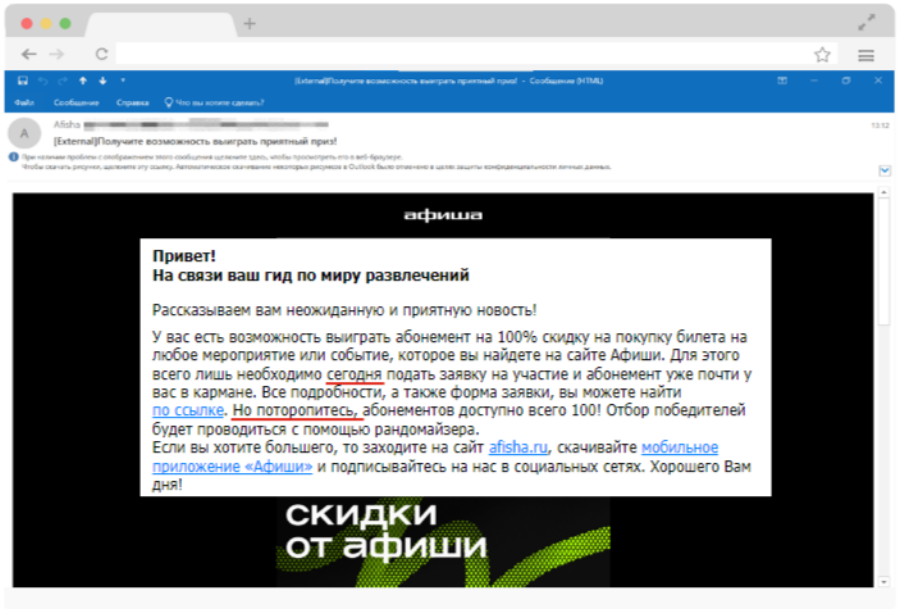
У отправителя письма подозрительный адрес



Как распознать фишинговое письмо

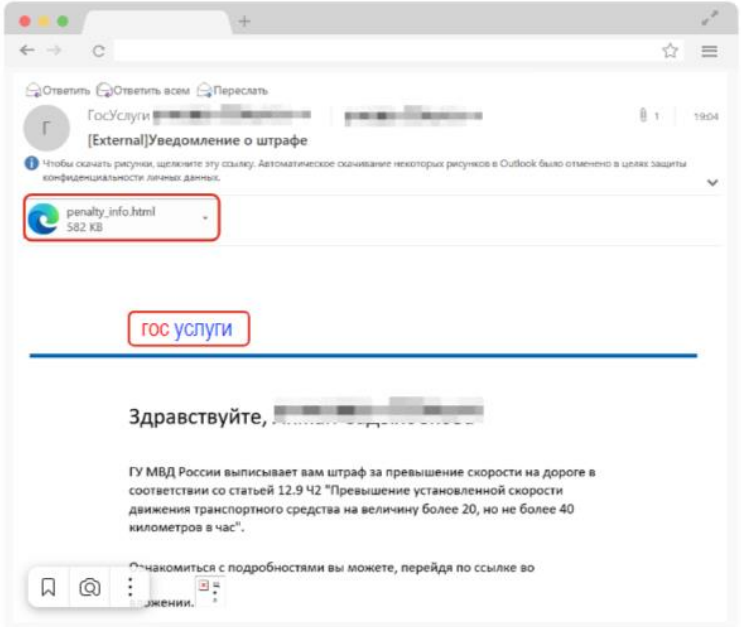
Письмо содержит призывы сделать что-то срочно:

- подтвердить перевод, ваш адрес или другие личные данные
- воспользоваться горящими акциями и предложениями, которые действуют «только сегодня»



Как распознать фишинговое письмо

У письма некачественная графика и странная верстка



Как защититься от фишинга

Подключите двухфакторную аутентификацию везде, где это возможно

Используйте защиту по двум параметрам: через логин и пароль, а также, например, по коду из СМС

Используйте сложные пароли

Чем длиннее пароль и чем более разнообразные символы в нем использованы, тем пароль надежнее

С осторожностью открывайте письма или сообщения от неизвестных отправителей, а также ссылки и вложения в таких письмах

А если все-таки открыли – немедленно сообщите в ИТ-отдел

Регулярно обновляйте софт

Хакеры могут использовать уязвимости программного обеспечения. Чтобы избежать проблем, регулярно устанавливайте обновления

Передавайте конфиденциальную информацию безопасно

Если вы работаете
с конфиденциальной информацией
(например, персональные данные),
запомните, как передавать ее
безопасно:

- Передавайте информацию в зашифрованном архиве
- Ключ отправьте по другому каналу связи (например, через мессенджер или по СМС)

Безопасность мобильных устройств

Небезопасная работа с мобильных устройств может стать причиной утечки информации организации и повлечь серьезные последствия.

Мобильные устройства сотрудника обычно используются в местах, не контролируемых организацией. Даже если устройства используются внутри офиса, они переносятся с места на место, что создает угрозу утечки конфиденциальных данных.

В этом курсе вы узнаете, как правильно и безопасно работать с мобильными устройствами

1. Следите за устройствами

В поездке и в общественном месте помните о безопасности устройств.

Не оставляйте смартфон или компьютер без присмотра

2. Блокируйте экран

Всегда блокируйте экран компьютера и смартфона, даже если отходите всего на минуту

Горячие клавиши для блокировки экрана компьютера

WIN + L

Оставить экран незаблокированным – то же, что оставить входную дверь открытой, чтобы незнакомцы могли войти и ограбить вас

3. Активируйте пароль или код на всех устройствах

Включите функцию блокировки вашего устройства

Тогда при множественном вводе неправильного пароля телефон заблокируется на некоторое время (от минуты до нескольких часов)

Также можно использовать функцию удаления данных при многократном неправильном вводе пароля. В случае потери или кражи вашего устройства мошенник не сможет получить доступ к нему

4. Активируйте функцию поиска

Включите функцию поиска устройства.

Настройте «Найти iPhone» или скачайте приложение Android Device Manager, чтобы иметь возможность заблокировать и/или стереть все данные удаленно

5. Будьте бдительны

Работая с телефона или планшета, пользуйтесь мобильной передачей данных 3G/LTE вместо подключения к неизвестным Wi-Fi-сетям. Если все же приходится использовать чужой Wi-Fi, выбирайте сети с защищенным подключением

При работе в публичных местах убедитесь, что в ваш экран никто не смотрит. Будьте особенно внимательны, если работаете с конфиденциальными данными

6. Подключите двухфакторную аутентификацию

Такой метод идентификации пользователя в каком-либо сервисе при помощи запроса аутентификационных данных двух разных типов обеспечивает двухслойную, а значит, более эффективную защиту аккаунта от несанкционированного проникновения.

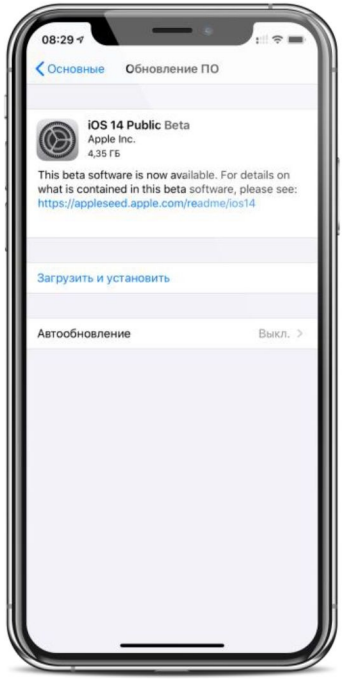
Например, для входа в аккаунт помимо пароля у вас запросят дополнительную информацию, например цифровой код, который отправляется по СМС/email или вычисляется через специальное приложение-аутентификатор на смартфоне

7. Регулярно обновляйте ПО

Разработчики программ устраняют уязвимости в программах и выпускают более защищенные версии. Настройте автоматические обновления

Необходимо регулярно обновлять:

- Операционную систему
- Браузер
- Антивирус
- Все рабочие программы



Физическая безопасность

Каждый день злоумышленники пытаются получить информацию различными способами.

Преодоление физической защиты организации – один из вариантов хакерской атаки.

Знание методов такой атаки и способов их предотвращения поможет сотруднику защитить организации

Как может происходить физическая атака

Действия злоумышленников

1

Разведка

Изучают информацию об организации, следят за сотрудниками в сети и за пределами офиса

2

Подготовка

На основе полученной информации продумывают легенду, выбирают время и место для операции, готовят технические средства

3

Операция

Проникают на территорию для физической атаки. Исполнитель обладает актерским талантом и обаянием

4

Целевое действие

Проводят физическую атаку: взламывают систему, крадут данные

Для реализации всех этапов атаки злоумышленники могут использовать:

Социальные сети

- Фото, которые сделаны в офисе, с отмеченными людьми, геолокацией, интересами
- Имена и другие личные данные (ваши и ваших коллег), которые в дальнейшем используют для создания правдоподобной легенды

Интернет

- Информацию о компании в профессиональных блогах и на форумах
- Переписку сотрудников в блогах и на форумах

Пропускную систему в офис

- Знания, как охрана относится к людям без пропуска
- Знания, как проходят в офис контрагенты и курьеры

Внутренняя угроза

Обратите внимание, что угрозу может представлять не только внешний нарушитель, но и внутренний. Например, сотрудник организации или обслуживающий персонал

Признаки, которые могут выдать внутреннего нарушителя:

Изменения в поведении, например снижение вовлеченности в трудовой процесс, рассеянность, посещение в рабочее время социальных сетей и развлекательных сайтов

Отклонения от стандартного алгоритма работы с информационными системами и данными

Как избежать физической атаки

1 Не публикуйте информацию об организации

Любой ваш пост о работе может помочь злоумышленникам в онлайн-разведке

Хакеры детально изучают фотографии, сделанные в офисе и опубликованные в сети, чтобы найти зацепки для атаки

Как избежать физической атаки

2 Не пропускайте посторонних

Ваш пропуск всегда должен находиться при вас. Никогда не передавайте его даже коллегам или посетителям, которых вы хорошо знаете

Не провожайте никого в офис, кем бы незнакомец ни представился. Обязательно отведите его в бюро пропусков и оповестите охрану. Незнакомец должен оформить пропуск надлежащим образом

Как избежать физической атаки

3 Оберегайте пропуск в офис

Будьте бдительны в общественных, местах и транспорте, если кто-то пытается подойти слишком близко

Используйте защитные RFID-чехлы для ношения пропуска. Они сделаны из металлизированного материала, который не позволит считать пропуск

Как избежать физической атаки

4 Не обсуждайте рабочие процессы с посторонними

Не сообщайте никому конфиденциальную информацию о клиентах и коллегах

Если неформальные разговоры о работе увлекли вас и вы по неосторожности раскрыли конфиденциальную информацию, срочно сообщите об этом в ИТ-отдел

Как избежать физической атаки

5 Всегда блокируйте экран компьютера и смартфона, если отходите даже на минуту

Блокировка экрана поможет избежать неправомерного воздействия со стороны внутреннего нарушителя

Горячие клавиши для блокировки экрана компьютера:

WIN + L

Оставить экран незаблокированным – то же, что оставить входную дверь открытой, чтобы незнакомцы могли войти и ограбить вас

Как избежать физической атаки

6 Активируйте пароль или код на всех устройствах

Установите автоблокировку на ваших устройствах

В случае потери или кражи устройства мошенник не сможет получить доступ к вашим данным

Как избежать физической атаки

7 Не подключайте к компьютеру неизвестные устройства

Если вы не знаете, что за флешка лежит на столе, не нужно подключать ее к компьютеру. Там может быть что угодно, в том числе программа, которая полностью уничтожит ваш компьютер

Отнесите незнакомое устройство в IT-ответ

Один из способов, которыми проверяют защищенность организации – подброшенные флешки с сюрпризом в виде вредоносной программы

Как избежать физической атаки

8 Сохраняйте порядок на рабочем столе

- Убирайте со стола в ящик документы, с которыми работаете
- Не оставляйте материалы на столе без присмотра
- Удаляйте с рабочего компьютера файлы, которые вам больше не нужны

Полиция вне офиса

Звонок из полиции

Если вам звонят на личный номер, предлагают пообщаться или даже явиться на допрос в качестве свидетеля, спросите, по какому делу, и свяжитесь с юристами организации

Обязательно сообщите о произошедшем в службу безопасности

Полиция вне офиса

Повестка из полиции

Если вам присылают повестку по почте и вызывают на допрос в качестве свидетеля, передайте повестку и все, что вам известно, в службу безопасности или юристам организации

Безопасная удаленная работа

Правила безопасной работы

Передавайте конфиденциальную информацию безопасно

Если вы работаете с конфиденциальной информацией, например, с персональными данными, запомните, как передавать ее безопасно:

- Пересылайте конфиденциальную информацию в зашифрованном архиве
- Ключ отправьте по другому каналу связи (например, через мессенджер или по СМС)

Если во время удаленной работы с вашего компьютера утекут конфиденциальные документы, отвечать придется именно вам.

Чтобы предотвратить такую возможность, нужно уметь безопасно работать вне офиса

Правила безопасной работы

1 Всегда блокируйте экран компьютера и смартфона, если отходите даже на минуту

Блокировка экрана поможет избежать неправомерного воздействия со стороны внутреннего нарушителя

Горячие клавиши для блокировки экрана компьютера:

WIN + L

Оставить экран незаблокированным – то же, что оставить входную дверь открытой, чтобы незнакомцы могли войти и ограбить вас

Правила безопасной работы

2 Не подключайте к компьютеру неизвестные устройства

Если вы не знаете, что за флешка лежит на столе, не нужно подключать ее к компьютеру. Там может быть что угодно, в том числе программа, которая полностью уничтожит ваш компьютер

Отнесите незнакомое устройство в IT-ответ

Один из способов, которыми проверяют защищенность организации – подброшенные флешки с сюрпризом в виде вредоносной программы

Правила безопасной работы

3 Используйте сложные пароли

Чем длиннее пароль, тем труднее его взломать. Исследования показывают, что чем длиннее пароль и чем более разнообразные символы в нем использованы, тем больше времени требуется для его взлома:

- Пароль 7468 взламывается моментально
- rutryicse–за 5 секунд
- LpjkfHKfdjl –за 5 лет
- 7VEKI3iiwivekk]U – за 93 триллиона лет

Кол-во символов	Только цифры	Строчные буквы	Заглавные и строчные буквы	Цифры, заглавные и строчные буквы	Цифры, заглавные и строчные буквы, символы
4	Сразу	Сразу	Сразу	Сразу	Сразу
5	Сразу	Сразу	Сразу	Сразу	Сразу
6	Сразу	Сразу	Сразу	1 секунды	5 секунды
7	Сразу	Сразу	25 секунды	1 минуты	6 минуты
8	Сразу	5 секунды	22 минуты	1 час	8 часов
9	Сразу	2 минуты	19 часов	3 дня	3 недели
10	Сразу	58 минуты	1 месяц	7 месяцев	5 лет
11	2 секунды	1 день	5 лет	41 год	400 лет
12	25 секунды	3 недели	300 лет	2 000 лет	34 000 лет
13	4 минуты	1 год	16 000 лет	100 000 лет	2 млн лет
14	41 минуты	51 год	800 000 лет	9 млн лет	200 млн лет
15	6 часов	1 000 лет	43 млн лет	600 млн лет	150 млрд лет
16	2 дня	34 000 лет	2 млрд лет	37 млрд лет	1 трлн лет
17	4 недели	800 000 лет	100 млрд лет	2 трлн лет	93 трлн лет
18	9 месяцев	23 млн лет	61 трлн лет	100 трлн лет	7 квлн лет

Правила безопасной работы

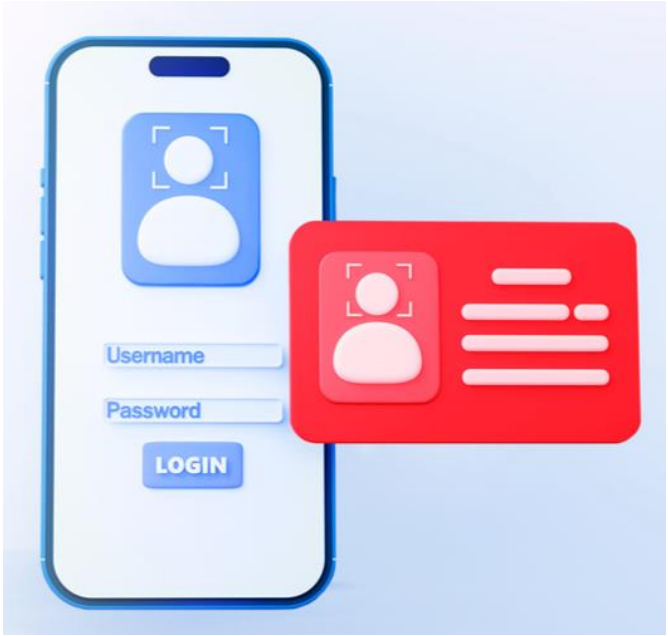
4 Подключите двухфакторную аутентификацию

Тогда для входа в аккаунт помимо пароля у вас запросят дополнительную информацию. Например, цифровой код, который отправляется по СМС/email или вычисляется через специальное приложение-аутентификатор на смартфоне

Правила безопасной работы

5 Выходите из всех аккаунтов

По возможности не заходите в свои учетные записи с чужих устройств. Если это все же необходимо, по завершении работы разлогиньтесь и закройте соответствующие вкладки



Правила безопасной работы

6 Один сайт – один пароль

Для каждого сайта должен быть уникальный пароль

Не используйте пароль от корпоративных систем на сторонних сайтах, в соцсетях, мессенджерах и т. д.

Правила безопасной работы

7 Не пользуйтесь общественным Wi-Fi

Работая с телефона или планшета, пользуйтесь мобильной передачей данных 3G/LTE вместо подключения к неизвестным Wi-Fi-сетям

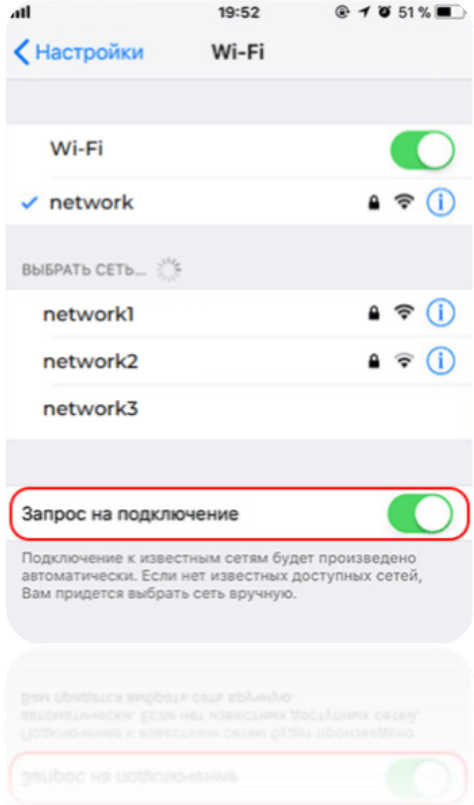
Если приходится использовать чужой Wi-Fi, выбирайте сети с защищенным подключением

Правила безопасной работы

8 Избегайте незнакомых сетей

Настройте уведомления о подключении ко всем новым Wi-Fi-сетям

Так ваш смартфон не подключится к посторонней сети без вашего подтверждения



Правила безопасной работы

9 Выходите в интернет безопасно

Работайте через VPN, когда находитесь вне офиса

Это защитит ваш интернет-трафик и скроет ваши личные данные при работе онлайн

Безопасность паролей

Безопасность паролей

Надежный пароль – главный барьер, который мешает взломать ваши аккаунты в сети. Если вы не пользуетесь современными методиками создания паролей, то, вполне вероятно, мошенники смогут подобрать ваши пароли буквально за несколько часов

Чтобы не подвергать себя риску кражи идентификационных данных и не стать жертвой вымогательства, вам нужно создавать пароли, которые могут противостоять усилиям хакеров, вооруженных современными средствами взлома

1. Никогда и никому не говорите свой пароль

Ваши учетные записи – ваша ответственность

Если злоумышленники украли ваш пароль, все действия, совершенные с вашей учетной записью, будут рассматриваться системами как действия, совершенные от вашего имени

Ваша учетная запись принадлежит только вам. Ни у кого не должно быть к ней доступа. Даже если у вас есть дополнительные учетные записи, они не должны быть доступны вашим коллегам

Не говорите и не высылайте свой пароль никогда и НИКОМУ, даже сотрудникам ИТ-отдела

2. Используйте менеджер паролей

Менеджер паролей – специальная программа для хранения паролей и логинов от учетных записей и для безопасной авторизации в интернете.
Главное преимущество: для доступа ко всем данным достаточно запомнить один мастер-пароль

Основные функции менеджера паролей:

- Хранение и передача паролей безопасным способом
- Генерация новых паролей
- Автозаполнение форм регистрации
- Хранение конфиденциальной информации
- Синхронизация между устройствами через защищенное облачное хранилище

3. Запоминайте пароли правильно

Как запомнить тяжелый пароль?

Воспользуйтесь мнемонической техникой при его создании, и вы сможете относительно легко его запомнить

Например:
MIsrvM@II:25 – «мой первый сын родился в Москве в 11:25»

Но! Не используйте:

Исходную фразу, слова или сочетания слов с добавлением различных символов

Какую-либо персональную информацию (даты, имена кумиров, клички питомцев)

4. Безопасно обращайтесь с паролями

Когда вы вводите пароль на сайте, браузер предлагает вам его запомнить. Это удобно. Но мы не рекомендуем этого делать: так вы рискуете передать свои учетные данные хакерам

Все пароли от важных систем надо менять на регулярной основе. Не стоит усложнять старый пароль, лучше создавайте совершенно новый

Используйте разные пароли для разных систем и сайтов. Если произойдет утечка учетных данных, вам нужно будет поменять только один пароль

5. Включите двухфакторную аутентификацию

Еще одно средство для усиления защиты вашей учетной записи – двухфакторная аутентификация (2FA). С ней для входа в систему вам нужно не только ввести пароль, но еще и предоставить дополнительную информацию

Это может быть цифровой код, который отправляется вам по СМС/email или вычисляется через специальное приложение-аутентификатор на вашем устройстве. Необходимо быть уверенным в безопасности приложения, прежде чем его устанавливать

Защита персональных данных

Ценность ПДн

Процветание организации тесно связано с тем, насколько серьезно она подходит к обеспечению информационной безопасности.

Особое значение имеют определение и нейтрализация угроз безопасности, касающихся несанкционированного доступа к персональным данным (ПДн) клиентов и партнеров.

Чтобы предотвратить утечку ПДн, нужно правильно обращаться с ними, знать их категории и правила обработки

Ценность ПДн

Коммерческая тайна

- Информация, которая имеет коммерческую ценность именно потому, что неизвестна никому другому
- Примеры: стратегические документы, технологические процессы, уникальные знания
- Для ее защиты в организации устанавливается режим коммерческой тайны. Предусмотрено привлечение сотрудников к ответственности за ее разглашение

Публичная информация

- Факты и сведения, доступ к которым не ограничивается
- Примеры: контактная информация, сведения о продуктах организации, информация на сайте и в пресс-релизах
- Нет требований к условиям хранения, передачи и уничтожения этого вида информации

Информация для внутреннего пользования

- Информация, которая используется во внутренних процессах организации всеми или некоторыми сотрудниками
- Примеры: отчеты, процедуры и положения
- Эта информация не должна передаваться за пределы организации

Ценность ПДн

Конфиденциальная информация

- Информация, доступ к которой есть только у тех, кто имеет на это право, и которую запрещено разглашать
- Каждая организация сама решает, какую информацию ей надо скрыть. В основном это ПДн и коммерческая тайна, а также вся информация, которая теряет ценность при разглашении
- Обычно процессы работы с конфиденциальной информацией детально прописаны, чтобы минимизировать риски ее утечки, а также обеспечить ее целостность и доступность для сотрудников, которые с ней работают. Зачастую применяются специальные условия хранения и шифрования при ее передаче

Персональные данные

- Информация, относящаяся к субъекту ПДн. Это информация обо всех людях, которые взаимодействуют с организацией: сотрудниках, клиентах, партнерах и т. д.
- В России действует закон о ПДн. За нарушения в сфере обработки и защиты ПДн может грозить ответственность – как административная, так и уголовная

Категории ПДн

Общедоступные ПДн

ПДн, которые размещены в открытом доступе

Специальные категории ПДн

- Расовая и национальная принадлежность
- Политические, религиозные и философские взгляды
- Сведения о здоровье и интимной жизни
- Сведения о судимости

Иные ПДн

Сведения, которые не относятся ни к одной из перечисленных категорий:

- Номер страхового свидетельства
- Серия и номер паспорта
- ИНН
- Адрес места жительства и др.

Биометрические ПДн

Сведения, которые характеризуют физиологические и биологические особенности человека и используются для установления личности:

- ДНК
- Отпечатки пальцев
- Сетчатка или радужка глаза
- Запись голоса
- Фото и др.

Основные понятия 152-ФЗ

Положения 152-ФЗ обеспечивают защиту прав и свобод человека при обработке ПДн, охраняют право на неприкосновенность частной жизни, а также личную и семейную тайну

Чтобы понять правила работы с ПДн, ознакомьтесь с основными понятиями этого закона:

1

ИСПДн (информационная система ПДн) – совокупность ПДн, содержащихся в базах данных, и обеспечивающих их обработку информационных технологий и технических средств

2

Обработка ПДн –любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение, извлечение, использование, передачу, обезличивание, блокирование, удаление, уничтожение ПДн. Любые действия с ПДн – это их обработка

Основные понятия 152-ФЗ

3

Оператор ПДн – государственный или муниципальный орган, физическое или юридическое лицо, которые обрабатывают ПДн. Оператор обязан обеспечить безопасную обработку ПДн. К организации, уполномоченной оператором ПДн, предъявляются те же требования по соблюдению конфиденциальности ПДн во время обработки, что и к оператору ПДн

4

Пользователи ПДн – все работники компании, участвующие в процессах обработки ПДн и допущенные к обработке ПДн. Если вы работаете с ПДн, вы относитесь к пользователям ПДн

5

Субъект ПДн – физическое лицо, ПДн которого обрабатываются оператором ПДн. Ваши сотрудники – это субъекты ПДн

Роль Роскомнадзора

- Функции регулирования в этой сфере, то есть установления правил и контроля их выполнения, осуществляет Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). Ее интересуют все случайные и неправомерные действия, которые привели к нарушению прав субъектов и нанесению им вреда. Операторы ПДн уведомляют Роскомнадзор о том, какие ПДн и с какой целью обрабатываются. Во внутренней документации оператора должны быть детально прописаны для каждой цели обработки: перечень ПДн, субъекты ПДн, сроки и порядок обработки

- С сентября 2022 года операторы ПДн должны уведомлять Роскомнадзор обо всех инцидентах безопасности с утечками данных, их причинах, предполагаемом вреде субъекту ПДн, принятых мерах, уполномоченном лице, которое от имени оператора взаимодействует с ведомством. Первое такое уведомление необходимо направить в течение 24 часов с момента обнаружения нарушения, а предоставить результаты внутреннего расследования – в течение 72 часов

Права Роскомнадзора

- Проверять сведения, которые ему предоставляют операторы ПДн
- Требовать от операторов блокирования или уничтожения полученных незаконным путем ПДн
- Ограничивать доступ к информации, которая обрабатывается с нарушением закона
- Обращаться в суд с исками по защите прав субъектов ПДн
- Направлять заявления о принятии мер по приостановлению действия или аннулированию лицензии оператора при соответствующих условиях
- Привлекать к ответственности лиц, нарушающих 152-ФЗ

С 1 сентября 2022 года ужесточились требования к операторам ПДн. Теперь вместо 30 у них есть всего 10 рабочих дней на выполнение следующих действий:

- Отрицательный ответ на запрос сведений о наличии обрабатываемых ПДн с разъяснением причин отказа
- Передача Роскомнадзору необходимых сведений по его запросу
- Ответ на обращение субъекта ПДн по поводу того, обрабатываются его данные или нет, а если да, то предоставление к ним доступа

Обработка ПДн

Это любая работа с ПДн в автоматизированном либо ручном режимах:

- Сбор
- Запись
- Систематизация
- Накопление
- Хранение
- Уточнение
- Извлечение
- Использование
- Передача
- Обезличивание
- Блокирование
- Удаление
- Уничтожение и др.

Меры защиты ПДн

1 Обращайтесь с паролями правильно

Чтобы злоумышленник не смог взломать ваше устройство или системы вашей компании:

- Создавайте сильные пароли
- Используйте менеджеры паролей
- Используйте специальные техники создания и запоминания паролей
- Подключите двухфакторную аутентификацию

Никому не передавайте пароли, как не даете никому ключи от своей квартиры. Даже если просят коллеги, руководитель или сотрудник ИТ-службы

Убедитесь, что все устройства, на которых вы работаете, защищены паролем

Меры защиты ПДн

2 Работайте в интернете безопасно

Вместо подключения к неизвестным сетям Wi-Fi используйте мобильный интернет

Не работайте на подозрительных сайтах

Пользуйтесь VPN

Проверяйте безопасность ссылок во входящих сообщениях

Обращайте внимание, куда вас направляет ссылка

Меры защиты ПДн

3 Безопасно устанавливайте программы

Чтобы не заразить компьютер или телефон вирусом:

Отказывайтесь от неожиданных предложений сайтов скачать и установить программу

Обновляйте программу только из интерфейса самой программы

Проверяйте безопасность приложения перед установкой его на телефон

Придерживайтесь правил организации при установке и обновлении программ

Меры защиты ПДн

4 Уничтожайте документы правильно

Для мобильных носителей используйте средства гарантированного уничтожения информации или самих носителей

Используйте шредер или другие устройства для уничтожения бумажных документов

Контролируйте печать документов

Меры защиты ПДн

5 Всегда блокируйте экран компьютера
и смартфона, если отходите даже на минуту

Блокировка экрана поможет избежать неправомерного воздействия со стороны внутреннего нарушителя

Горячие клавиши для блокировки экрана компьютера:

WIN + L

Оставить экран незаблокированным – то же, что оставить входную дверь открытой, чтобы незнакомцы могли войти и ограбить вас

Меры защиты ПДн

6 Храните документы в безопасности

Все шкафы, сейфы, помещения и хранилища, где хранятся документы с ПДн, должны быть заперты

Доступ к ним должен быть ограничен посторонним лицам

Все съемные носители, личные дела, флешки также должны храниться в защищенном месте

Меры защиты ПДн

7 Защитите себя от фишинга

Проверяйте входящие сообщение по списку:

1. Письмо неожиданное
2. Отправитель незнаком
3. Сообщение вызывает эмоцию
4. Есть акцент на срочность или авторитет
5. В письме есть потенциальное оружие (вложенные файлы, картинки, ссылки на сайты, странные просьбы)

Если есть совпадения хотя бы по 2 пунктам из списка, то не предпринимайте действий, о которых вас просят в сообщении, и перешлите его в ИТ-отдел

Ответственные при обработке ПДн

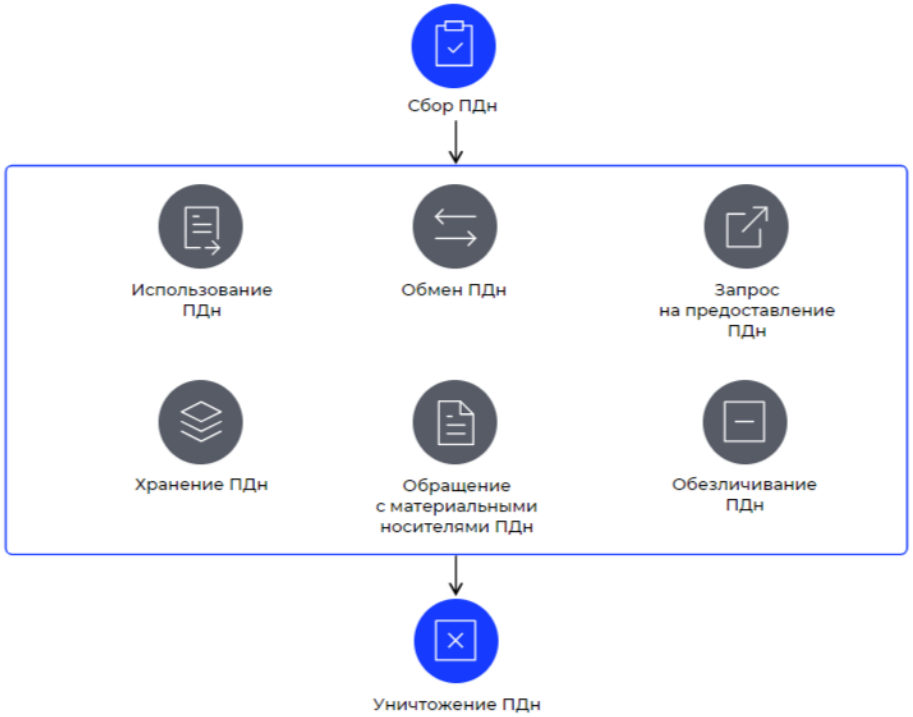
Ответственные за организацию обработки ПДн:

- Контролирует соблюдение требований законодательства РФ в области обработки ПДн
- Доводит до сведения сотрудников положения законодательства РФ в области обработки ПДн

Ответственные за обеспечение безопасности ПДн:

- Организует работу по созданию системы защиты ПДн, по подготовке внутренних документов в этой сфере
- Контролирует выполнение мер защиты ПДн

Основные правила работы с ПДн



Принципы работы с ПДн

Соответствие целям

Обрабатывать ПДн только в обозначенных целях, а также обрабатывать только ПДн, необходимые для выполнения цели

Прозрачность

Предоставлять субъектам всю информацию о том, какие ПДн компания собирает, как и зачем их обрабатывает

Достоверность

Поддерживать все обрабатываемые ПДн в актуальном состоянии

Ограничение хранения ПДн

Хранить безопасно ПДн только в течение необходимого времени

Безопасность

Предоставлять доступ к ПДн только тем, кто работает с ними

Основания обработки ПДн

С согласия субъекта ПДн оператор может поручить обработку ПДн третьей стороне на основании заключаемого с ней договора. Перечень ПДн и действий с ними, а также цели обработки ПДн определяются в поручении оператора ПДн. Организация, которая обрабатывает ПДн по поручению оператора, обязана обеспечить выполнение требований договора, в том числе конфиденциальность ПДн, которые получает от оператора

Организация, обрабатывающая ПДн по поручению оператора, не обязана получать согласие субъекта на обработку данных. Получение такого согласия – задача оператора ПДн

Компания, обрабатывающая ПДн по поручению оператора, обязана:

- Уведомлять оператора ПДн обо всех выявленных случаях нарушений обработки ПДн, а также о случаях нарушения доступа к ПДн
- По запросу оператора предоставлять информацию о порядке обработки, мерах защиты ПДн

Основания обработки ПДн

Перед сбором ПДн нужно, чтобы субъект этих данных подписал согласие на обработку ПДн

В согласии указываются:

- Фамилия, имя, отчество, адрес субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе
- Фамилия, имя, отчество, адрес представителя субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта ПДн)
- Наименование или фамилия, имя, отчество и адрес оператора, получающего согласие субъекта ПДн
- Цель обработки ПДн
- Перечень ПДн, на обработку которых дается согласие субъекта ПДн
- Наименование или фамилия, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению оператора, если обработка будет поручена такому лицу
- Перечень действий с ПДн, на совершение которых дается согласие, общее описание используемых оператором способов обработки ПДн
- Срок, в течение которого действует согласие субъекта ПДн, а также способ его отзыва, если иное не установлено 152-ФЗ
- Подпись субъекта ПДн

Бывают случаи, когда обработка ПДн возможна без согласия субъекта ПДн: для выполнения требований законодательства РФ или исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн, и др.

Права субъекта ПДн

Имеет право на получение информации, касающейся обработки его ПДн

Вправе обжаловать действия или бездействие оператора в уполномоченном органе по защите прав субъектов ПДн или в судебном порядке в случае, если считает, что оператор осуществляет обработку его ПДн с нарушением требований 152-ФЗ

Имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке

Согласие субъекта ПДн

Только с письменного согласия субъекта ПДн осуществляются:

- Обработка специальных
- и биометрических ПДн
- Трансграничная передача ПДн
- Распространение ПДн
- Передача ПДн работника третьим лицам
- Включение ПДн
- в общедоступные источники ПДн
- Принятие решения, порождающего юридические последствия в отношении субъекта ПДн, на основании исключительно автоматизированной обработки его ПДн

Равнозначным содержащему собственноручную подпись субъекта ПДн согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью

В остальных случаях закон допускает оформление согласия в любой иной форме, позволяющей подтвердить факт его получения оператором, например проставление галочки напротив текста о предоставлении согласия на сайте при регистрации

Кто обрабатывает ПДн

Оператор ПДн – тот, кто обрабатывает ПДн. Он несет ответственность за незаконную обработку ПДн. Это могут быть государственный или муниципальный орган, физическое или юридическое лицо.

Субъект ПДн –тот, чьи ПДн обрабатываются. Это могут быть сотрудники, кандидаты на трудоустройство, клиенты, партнеры, контрагенты, посетители сайтов организации и др.

Работа с электронной подписью

Информация становится документом только после того, как ее удостоверили – добавили к ней что-то, что позволяет проверить ее подлинность, а также исключить возможность подделки.

Самый привычный способ удостоверить документ – подписать его

Роль подписи

Благодаря подписи распечатка становится документом. Помимо удостоверяющей функции подпись может защищать документ от подделки

Задачи, которые решает подпись:

Превращает просто информацию в документ

Удостоверяет информацию

Подтверждает личность человека, который подписал документ

Защищает документ от подделки

Электронная подпись

Электронный документ состоит из нулей и единиц. Чтобы удостоверить его, идентифицировать подписанта и защитить документ от подделки, были разработаны специальные математические алгоритмы. Результат их работы – последовательность символов, сформированная на базе содержимого электронного документа

Особенность алгоритмов для формирования электронной подписи состоит в том, что результат их работы сильно зависит от содержания документа. Стоит изменить всего один символ (например, убрать точку или запятую) – и подпись получится совсем другой

Электронная подпись

Алгоритм удостоверения электронных документов использует для формирования подписи не только содержимое документа, но и уникальный ключ подписанта – сформированную по определенным правилам последовательность цифр. Использование другого ключа для подписи документа изменит подпись

В результате работы алгоритма получается электронная подпись, которая определяется содержимым электронного документа и ключом подписанта. Таким образом, электронная подпись защищает документ от подделки и удостоверяет подпись человека, которому принадлежит ключ

Преимущества электронной подписи

Необходима для электронного документооборота. Он невозможен, если нет хотя бы простой электронной подписи, но обычно нужна неквалифицированная или квалифицированная подпись

Без нее юрлица и ИП не смогут зарегистрироваться и работать в различных государственных системах, например в системе госзакупок или маркировки товаров

Ее нельзя подделать, то есть создать аналогичную комбинацию символов

За счет использования методов шифрования (кодирования) информации значительно повышает уровень кибербезопасности при обмене документами

Позволяет подписывать документы и обмениваться ими онлайн. Это особенно важно, когда отправить и получить документ нужно быстро

Ключи электронной подписи

- Ключ, с помощью которого формируется электронная подпись документа, позволяет переподписать его заново после внесения изменений. Это значит, что передавать такой ключ посторонним нельзя

- С помощью алгоритмов, в которых используется пара ключей (публичный и секретный), можно проверить подлинность электронной подписи

- Секретный ключ используется для подписи и шифрования документа. Публичный ключ позволяет расшифровать документ и проверить подлинность подписи

- Публичный и секретный ключи связаны между собой, однако вычислить по публичному ключу секретный невозможно. Чтобы проверить подлинность электронной подписи документа, требуется открытый ключ подписанта

Ключи электронной подписи

Для упорядочивания обмена ключами и выпуска новых ключей существуют специальные организации или подразделения в крупных компаниях – удостоверяющие центры

Чтобы защитить открытые ключи от модификации и подтвердить их подлинность, удостоверяющие центры подписывают их своей подписью

Открытый ключ с подписью удостоверяющего центра называется сертификатом открытого ключа. Именно сертификаты открытых ключей обычно используются при работе с электронной подписью

Хранение ключей

Особенности работы алгоритма электронной подписи определяют требования к хранению ключевой пары:

- Секретный ключ нужно хранить так, чтобы никто не имел к нему доступа, поскольку он позволяет подписать любой документ и любое письмо от вашего имени
- Открытый ключ или его сертификат можно хранить как угодно, в том числе пересылать коллегам, контрагентам и всем, кому может потребоваться проверить подлинность вашей подписи
- Чтобы никто не мог похитить секретный ключ электронной подписи, нужно хранить его особым образом. Флешка, реестр компьютера или папка на диске не подойдут – они не имеют защиты от несанкционированного доступа
- Для безопасного хранения секретных ключей были разработаны специализированные устройства – токены

Токены

Токен содержит защищенную паролем память, прочитать которую можно только с помощью специальных программ. Таким образом, посторонний не сможет воспользоваться вашим секретным ключом и подписать документ вашей подписью

Внешне токен напоминает USB-флешку: подобно ей, он подключается к USB-порту. Но на этом сходство заканчивается

Правила использование электронной подписи

Согласно 63-ФЗ, электронная подпись – аналог собственноручной. Это значит, что электронные документы, подписанные вашей электронной подписью, имеют такую же юридическую силу, как и бумажные, подписанные собственноручно

Чтобы исключить риски, связанные с несанкционированным использованием вашей электронной подписи, нужно соблюдать правила ее безопасного использования

Правила использование электронной подписи

1. Храните электронную подпись только на специальных защищенных носителях – токенах

2. Защищайте токен от несанкционированного использования паролем. Измените стандартный пароль при первом использовании

3. Работайте с ключами электронной подписи только на выделенных для этого рабочих местах

4. Извлекайте токен из USB-порта компьютера, когда не работаете с ним

5. Храните токен в сейфе или защищенном шкафу

6. Не передавайте токен другим людям

7. Не выносите токен за пределы офиса

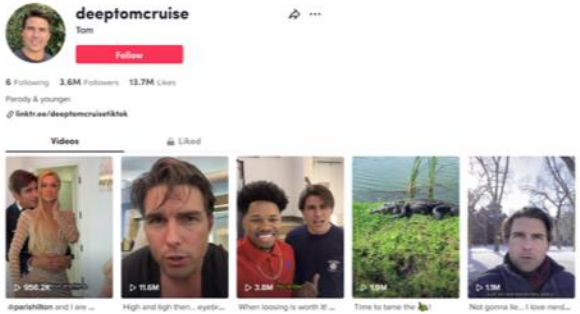
Дипфейк

Каждый день мошенники изучают новые инструменты и методы взлома.

Дипфейк – инструмент, который недавно появился в арсенале злоумышленников. С помощью него можно манипулировать общественным мнением, создавать путаницу и раздоры, распространять фейковые новости и ложную информацию, генерировать поддельные изображения и видео

Технология дипфейка

Дипфейк (от англ, deepfake) использует глубокое машинное обучение для создания изображений, видео- или аудиозаписей, имитирующих события. Обычно мошенники дублируют чей-то голос и/или черты лица и вставляют их в существующую запись или фотографию



На скриншоте выше показан пример дипфейка в соцсети. Аккаунт DeepTomCruise публикует неотличимые от настоящих дипфейк-видео с Томом Крузом. Ролики сразу начали набирать популярность за счет своей реалистичности

Голосовой дипфейк

Возможности для создания дипфейков практически безграничны – начиная с простых развлекательных приложений и онлайн-курсов и заканчивая программами вроде DeepFaceLab и компаниями, которые принимают заказы на фейки. Если раньше системам требовались десятки или даже сотни часов звука, то теперь – всего несколько минут аудиоконтента. При этом уже есть возможности, чтобы добавлять в искусственную речь эмоции

Для синтеза голоса сервису достаточно нескольких часов исходных аудиоданных, озвученных обладателем голоса. Программа создаст реалистичное озвучение требуемого текста

Голосовой дипфейк для мошенников

Сама суть технологии делает ее идеальным инструментом для злоумышленников

В 2020 году в британском исследовании Dawes Centre for Future Crime киберпреступления с использованием дипфейка были признаны одними из самых опасных. В отчете Recorded Future за апрель 2021 года спрогнозировали увеличение случаев использования дипфейка для использования в цифровых атаках

Дипфейк-фишинг – это попытка подделать личность в целях манипуляции другими людьми и получения от них доступа к финансам или конфиденциальной информации

Научитесь распознать дипфейк

Существует несколько признаков, по которым можно определить поддельное видео

1 Глаза и артикуляция

Блики в глазах не совпадают, сами глаза не двигаются либо двигаются неестественно. Человек не моргает, лицо замирает на доли секунды – это происходит при искусственной склейке кадров.

Сюда же относится сбитая артикуляция, когда дикция дипфейка не соответствует произносимым словам

Научитесь распознать дипфейк

2 Качество картинки

Неестественный тон кожи, освещение, неправильные тени – все это свойственно дипфейкам.

Также подделки не смогут точно воссоздать волосы и зубы – чаще всего они будут статичными и размытыми

Научитесь распознать дипфейк

3 Искаженные контуры лица

Важный критерий – размазанная картинка на стыке головы и шеи. Также часть лица (например, подбородок или нос) может быть размазана.

Любой блюр на видео – повод задуматься о его оригинальности

Правила чистого стола и чистого экрана

Чистые рабочий стол и экран – это не только эстетический фактор, но и важный элемент кибербезопасности.

Чтобы снизить риск несанкционированного использования информации, необходимо соблюдать правила чистого стола и чистого экрана

1. Сохраняйте рабочий стол чистым

Любой оставленный на столе документ могут украсть, сфотографировать или увидеть те, кому это не предназначено

Храните все документы и съемные носители в закрытых ящиках стола или шкафах

Не оставляйте документы на столе, если не работаете с ними прямо сейчас

2. Используйте сложные пароли

Чем длиннее пароль, тем лучше

Надежный пароль–главный барьер, который мешает взломать ваши устройства и аккаунты.

Для запоминания паролей используйте собственную память или менеджер паролей.

Не записывайте ваши пароли на листочках

3. Уничтожайте бумажные документы правильно

Используйте шредер, чтобы уничтожать бумажные документ

Копии документов с конфиденциальной информацией могут попасть в руки мошенников и использоваться в рамках атаки на вас или компанию

Не дайте злоумышленникам шанс найти что-то в мусоре

4. Удаляйте ненужные электронные документы

Ненужные файлы – это цифровой мусор, который мешает безопасной работе

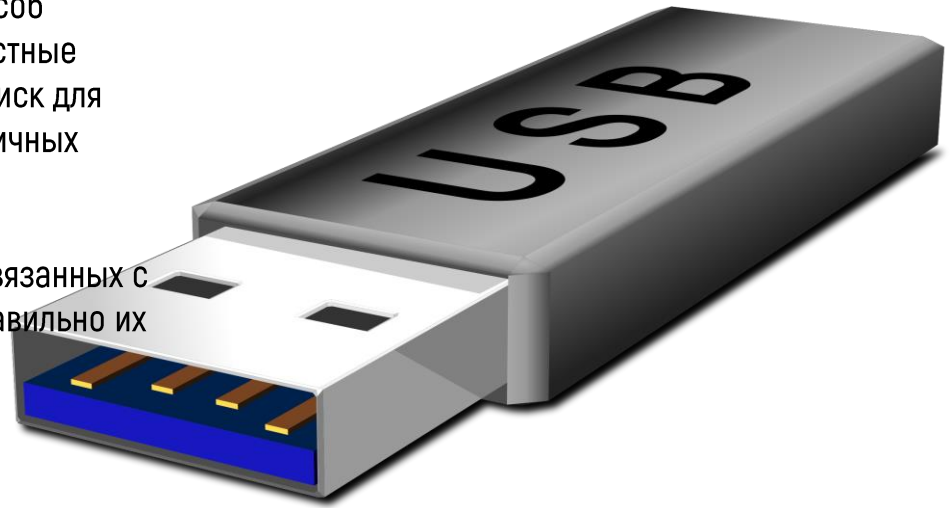
Удаление файлов, которые устарели или более не нужны, снижает вероятность их несанкционированного использования или утечки информации

Кроме того, удаление мусора и очистка кеша помогают удалить файлы, которые могут потенциально повредить систему компьютера

Неизвестные USB-устройства

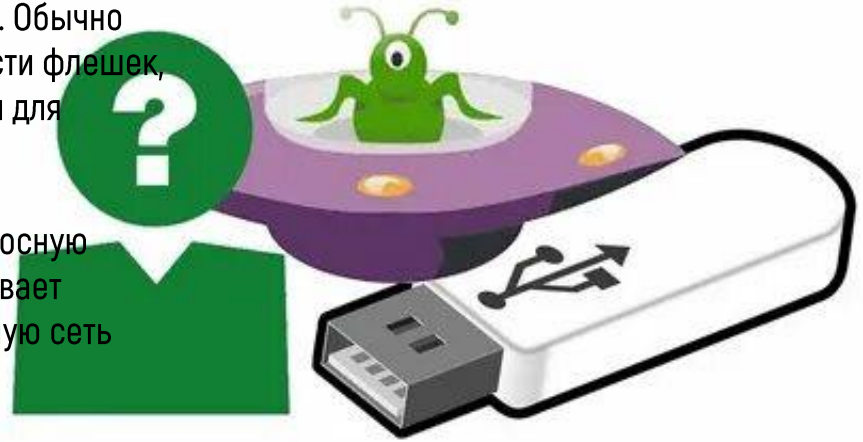
USB-устройства –удобный и популярный способ передачи и хранения данных. Однако неизвестные носители информации представляют собой риск для безопасности вашего компьютера и ваших личных данных.

Чтобы защитить себя и компанию от угроз, связанных с USB-устройствами, необходимо знать, как правильно их использовать



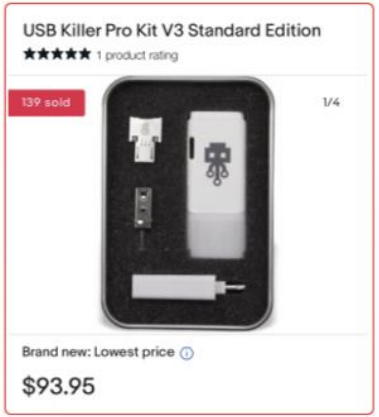
Неизвестное устройство – это всегда угроза

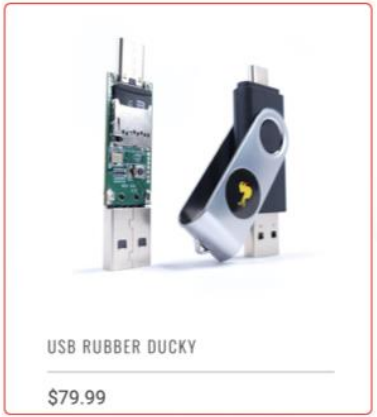
- Подброшенные флешки с вредоносной программой – работающий способ взлома компьютера. Обычно сотрудники не задумываются об опасности флешек, поэтому их часто используют мошенники для реализации атак на организацию
- Любая флешка может содержать вредоносную программу вроде BadUSB, которая открывает злоумышленникам доступ в корпоративную сеть компании через ваш компьютер



Устройства-киллеры

В свободной продаже есть флешки-убийцы, которые могут уничтожить ваш компьютер





С помощью простых технологий злоумышленники могут захватить контроль:

- Над компьютером, если к нему подключен кабель от дополнительного устройства
- Над беспроводной мышью или клавиатурой – без непосредственного доступа к ним, на расстоянии до 100 метров
- Над телефоном при его подключении к взломанной станции для подзарядки в общественном месте

Защитите себя и организацию

1 Не подключайте неизвестные флешки и другие USB-устройства к вашему рабочему компьютеру, даже если:

- Вы нашли их в офисе или на своем столе
- Кто-то прислал их вам по почте
- Они выглядят мило

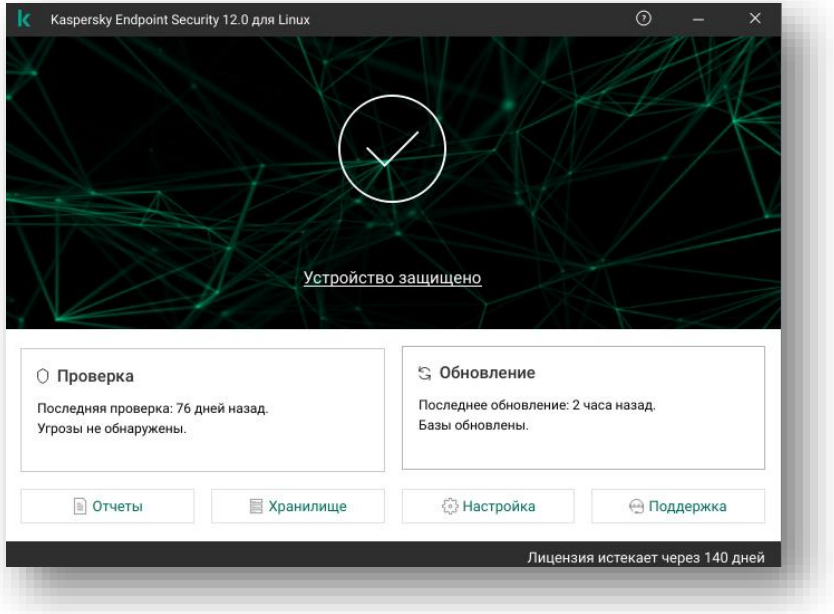
Такое устройство способно быстро заразить не только ваш компьютер, но и всю систему организации

Если вы подключите зараженное устройство к своему компьютеру, мошенники смогут получить доступ к каждому нажатию вашей клавиши и развертывать другие вредоносные программы по своему желанию, оставляя вас без защиты

Защитите себя и организацию

2 Сканируйте устройства

Если вам нужно использовать USB-носитель, перед запуском обязательно просканируйте его на наличие вредоносных программ с помощью антивирусного ПО или специальных программ



Защитите себя и организацию

3 Извлекайте USB-устройства правильно

Извлекайте устройства безопасно, следуя инструкциям вашей операционной системы, чтобы избежать повреждения данных или оборудования

Защитите себя и организацию

4 Соблюдайте правила работы с личными и рабочими USB-устройствами

Не используйте личные устройства в вашей рабочей системе или на корпоративном ПК. Это предотвратит распространение вредоносного ПО на всю сеть

Храните рабочие USB-носители в надежном месте и не давайте ими пользоваться посторонним лицам

Защитите себя и организацию

5 Отключите функцию автозапуска на компьютере

Эта функция предназначена для обнаружения и автоматического запуска любого USB-устройства, CD или DVD, вставленного пользователем

К сожалению, удобный инструмент может стать угрозой, если на съемном устройстве присутствует вредоносный код, который может быстро распространиться на всю систему

Защитите себя и организацию

6 Используйте пароли для доступа к своим USB-устройствам

Использование паролей на устройствах поможет предотвратить кражу данных

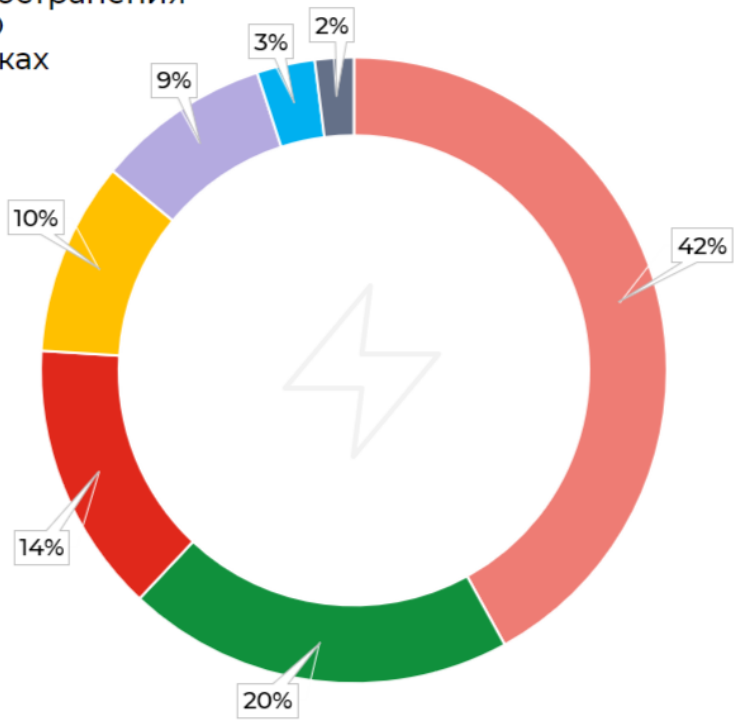
Социальные сети

Около 60% сведений, необходимых злоумышленнику для проведения атаки, можно легко найти, используя только социальные сети.
Вооружившись общедоступной информацией, киберпреступник может составить ваш социальный портрет и использовать его в бесчисленных попытках проникнуть во внутреннюю сеть вашей компании.

Чтобы не дать такую возможность злоумышленнику, следуйте правилам безопасного использования социальных сетей

Статистика

Способы распространения шпионского ПО в успешных атаках на частных лиц



- Сайты
- Электронная почта
- Социальные сети
- Официальные магазины приложений
- Мессенджеры и СМС-сообщения
- Компрометация компьютеров, серверов и сетевого оборудования
- Другие

14% успешных атак приходится на социальные сети

Статистика

Всего 1/3
россиян воздерживается от обсуждения работы в соцсетях

Остальные не видят ничего опасного в том, чтобы процитировать рабочую переписку в мессенджерах, выложить ее скриншот или обсудить рабочие новости со знакомыми.

В опросе* приняли участие более 3 тысяч респондентов из всех регионов

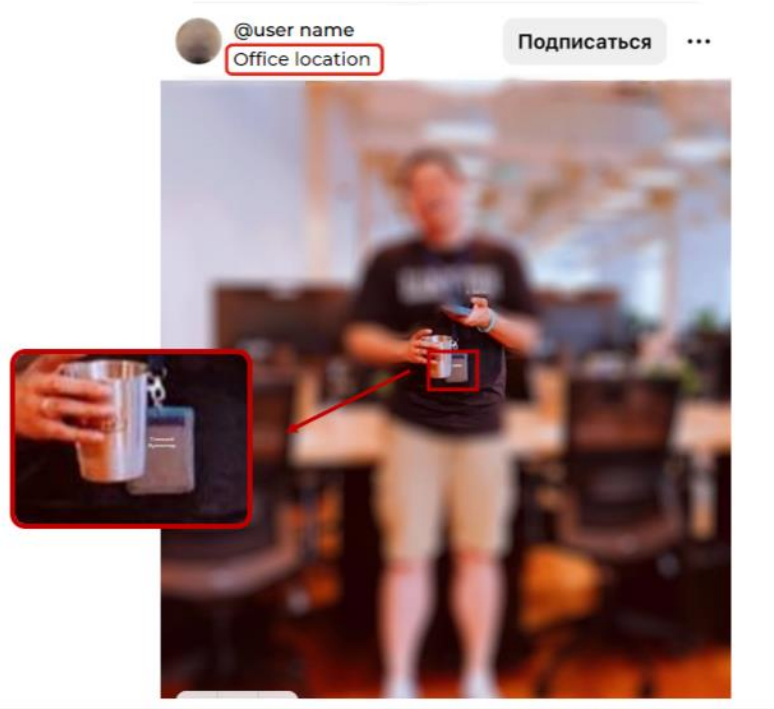
*По данным аналитического центра «АльфаСтрахование

1. Подумайте дважды, прежде чем что-то публиковать

Информация, которую может получить злоумышленник из социальных сетей:

Местоположение компании
Ваши должностные обязанности
Рабочий адрес электронной почты
Скриншоты бесед
Номера телефонов и адреса
Ваше финансовое положение

Не публикуйте ничего из этого списка, чтобы предотвратить атаку на сотрудников и компанию



2. Не оставляйте цифровой след

Не публикуйте внутреннюю информацию о компании в социальных сетях

Любой ваш пост о работе на внешних площадках может помочь злоумышленникам при онлайн-разведке

Решение – перенести публикации и общение в закрытые рабочие мессенджеры и системы

3. Не публикуйте конфиденциальную информацию

Никогда не делитесь с конфиденциальной информацией

1. О клиентах
2. Сотрудниках
3. Разработках организации
4. Бухгалтерской отчетности
5. Структуре организации
6. Сделках
7. Рабочих проектах
8. Системах защиты

Этапы атаки через социальные сети

Этап 1

Сбор данных

Злоумышленник собирает данные о персонале из открытых источников, а также информацию о возможных уязвимостях в защите: проводных и беспроводных сетях, настройках оборудования.
На первом шаге киберпреступнику доступны только данные, которые может найти любой пользователь интернета

Этап 2

Сканирование

На этом этапе злоумышленник ищет способы проникнуть в сеть и найти более конфиденциальную информацию – проверяет IP-адреса, аккаунты и идентификационные данные сотрудников

Этап 3

Получение доступа и атака на компанию

Дальше злоумышленник использует все средства для попадания во внутреннюю сеть и кражи информации.
Он рассылает поддельные письма по корпоративным адресам, чтобы выявить сотрудников, склонных доверять непроверенной информации

Кибератаки и способы защиты от них

Кибератака – это несанкционированный доступ к информационной системе / компьютерной сети

Успешная атака может спровоцировать утечку данных, что приведет к их краже или манипулированию ими. В результате организации несут финансовые потери, подрывается доверие клиентов, наносится репутационный ущерб

Чтобы атаки не приводили к подобным последствиям, нужно знать, каких видов они бывают и как правильно защитить от них себя и организацию

1. Почтовый фишинг

Что это

Атака с помощью методов социальной инженерии, при которой злоумышленник выдает себя за доверенное лицо или организацию и отправляет жертве поддельные электронные письма

Как реализуется

Не зная о том, что письмо мошенническое, жертва открывает его и переходит по вредоносной ссылке или открывает вложение.
В итоге злоумышленник получает доступ к конфиденциальной информации и учетным данным. Он также может установить вредоносное программное обеспечение (вредоносное ПО) на устройство жертвы

Меры защиты

1. Внимательно изучайте электронные письма, которые вы получаете. Большинство фишинговых писем содержат орфографические ошибки и изменения формата
по сравнению с оригинальными
2. Не переходите по ссылкам в письме
3. Не загружайте файлы, прикрепленные к письму от неизвестного отправителя
4. Обновляйте почту и браузер на постоянной основе
5. Регулярно меняйте пароли

2. Голосовой фишинг (вишинг)

Что это

Разновидность социальной инженерии, использующая технологию голосовой связи

Как реализуется

Мошенники используют телефонные звонки или голосовые сообщения, чтобы выдать себя за настоящие компании и обманом заставить вас перевести им деньги или раскрыть личную информацию

Меры защиты

1. Не отвечайте на телефонные звонки с неизвестных номеров
2. При малейшем подозрении кладите трубку и самостоятельно перезванивайте в организацию, из которой якобы звонят, по номеру с официального сайта
3. Никогда не сообщайте посторонним людям личную информацию, такую как номера банковских счетов, паспортные данные, СНИЛС, ИНН, пароли и коды двухфакторной аутентификации
4. Проверьте номер, с которого вам звонят, через интернет-поисковики
5. Мошенники будут вас торопить, но сделайте паузу, подумайте дважды, прежде чем что-то предпринимать

3. СМС-фишинг (смишинг)

Что это

Атака с помощью методов социальной инженерии, в которой используются поддельные СМС-сообщения. Их цель – обманом заставить людей загрузить вредоносное ПО, поделиться конфиденциальной информацией или отправить деньги киберпреступникам

Как реализуется

Злоумышленник отправляет жертве текстовое сообщение якобы от законного источника, например госучреждения, банка или известной компании.
Сообщение вызывает ощущение срочности или интереса и вынуждает жертву перейти по фишинговой ссылке или загрузить вредоносный файл.
Мошенники также могут выдавать себя за службу поддержки, начальника, коллегу или родственника

Меры защиты

1. Не отвечайте на сообщения с неизвестных номеров
2. Не переходите по ссылкам в сообщении, не открывайте и не скачивайте вложения
3. Проверяйте номер, с которого пришло СМС-сообщение, через интернет-поисковики
4. Блокируйте номер телефона, с которого пришло подозрительное СМС-сообщение

4. Атаки через социальные сети

Что это

Атака с помощью социальной инженерии, при которой злоумышленник использует информацию из открытых источников

Как реализуется

Около 60% информации, необходимой злоумышленнику
для проведения атаки, он находит в социальных сетях.
Потом киберпреступник составляет социальный портрет и использует его в бесчисленных попытках проникнуть во внутреннюю сеть организации

Меры защиты

1. Не делитесь конфиденциальной информацией в соцсетях
2. Не принимайте запросы на добавление в друзья от неизвестных людей, даже если у вас есть общие с ними друзья
3. Регулярно меняйте пароли
4. Не используйте одинаковые пароли для разных аккаунтов

Кейс

На фото, которое опубликовала сотрудница в соцсети, попала конфиденциальная информация, что привело к утечке данных компании

5. Программы-вымогатели

Что это

Тип атаки с помощью вредоносного ПО для заражения устройства жертвы – компьютера, принтера, смартфона, носимого устройства или другой конечной точки

Как реализуется

Злоумышленник блокирует и шифрует данные жертвы, важные файлы, а затем требует оплату за разблокировку и расшифровку данных

Меры защиты

1. Используйте антивирусное программное обеспечение
2. Делайте резервное копирование данных
3. Будьте бдительны и не переходите по подозрительным ссылкам
4. Регулярно обновляйте операционную систему, браузеры и другие приложения
5. Немедленно сообщайте в ИТ-отдел об инциденте

Примеры программы-вымогателя

Страх перед коронавирусной инфекцией (COVID-19) широко использовался киберпреступниками.

Программа-вымогатель CovidLock заражает устройства жертв через вредоносные файлы, обещая предоставить больше информации о болезни

После установки CovidLock шифрует данные с устройств Android и запрещает жертвам доступ к ним. Чтобы его вернуть, нужно заплатить выкуп в размере 100 долларов

6. Брутфорс-атака (атака грубой силой, или атака полным перебором)

Что это

Метод взлома, при котором злоумышленник подбирает разные варианты логинов, паролей и ключей шифрования для получения доступа к защищенным данным

Как реализуется

Злоумышленник применяет различные программы, инструменты или систематический перебор всех возможных комбинаций, пока одна из них не окажется верной. Чтобы угадать пароль, он может использовать так называемые словари паролей, которые содержат уже известные пользовательские комбинации символов

Меры защиты

1. Используйте двухфакторную аутентификацию
2. Увеличьте длину и сложность пароля, используя буквы в различном регистре, цифры, а также специальные символы
3. Регулярно меняйте пароли
4. Используйте разные пароли для разных аккаунтов

7. Wi-Fi-атака

Что это

Кибератака, при которой третья сторона перехватывает сообщения между двумя участниками. Вместо того чтобы данные передавались напрямую между сервером и клиентом, эта связь разрывается злоумышленником

Как реализуется

После перехвата соединения злоумышленник может подменить сайт, на который вы переходите, получить доступ к вашим контактам, личным сообщениям, паролям и т. д. Злоумышленник также может подделать кнопку «Забыли пароль?» и сбросить ваши учетные данные, заблокировав вам доступ ко всем учетным записям

Меры защиты

1. Не подключайтесь к общественным сетям
2. Используйте двухфакторную аутентификацию
3. Увеличьте длину и сложность пароля, используя буквы в разном регистре, цифры и специальные символы
4. Регулярно меняйте пароли
5. Не используйте одинаковые пароли для разных аккаунтов

8. Атака «услуга за услугу»

Что это

Низкоуровневая форма взлома, основанная на социальной инженерии

Как реализуется

Злоумышленники звонят по случайным номерам, утверждая, что они из службы техподдержки, и предлагают какую-либо помощь.
Если человеку действительно нужны подобные услуги, мошенники «помогают» решить те или иные проблемы и в итоге получают доступ к устройству жертвы или возможность запускать вредоносное ПО

Меры защиты

1. Никогда не предоставляйте свою личную информацию
2. Всегда подвергайте сомнению подозрительные предложения
3. Обновляйте антивирусное программное обеспечение на своих устройствах

9. Scareware

Что это

Тактика кибератаки, при которой злоумышленник пугает людей якобы посещением поддельных либо зараженных сайтов или загрузкой вредоносного программного обеспечения

Как реализуется

Атака пугающего ПО часто запускается через всплывающие окна. Они появляются на экране пользователя, предупреждая о том, что его компьютер или файлы были заражены, а затем предлагая решение.
Атака направлена на то, чтобы напугать людей и заставить их платить за ПО, которое якобы обеспечивает быстрое решение «проблемы»

Меры защиты

Используйте ПО только от официальных поставщиков
2. Игнорируйте все неожиданные всплывающие окна, предупреждения о новых вирусах или предложения загрузить бесплатное ПО
3. Никогда не нажимайте кнопку «Загрузить» и всегда осторожно закрывайте объявления
4. Используйте блокировщики всплывающих окон и фильтры URL-адресов
5. Сообщайте в ИТ-отдел об инцидентах

10. Атака drive-by download

Что это

Вредоносные атаки, происходящие при посещении пользователем взломанных киберпреступниками сайтов или при попытке открыть зараженное HTML-сообщение в электронной почте

Как реализуется

Киберпреступники обычно используют автоматические запросы элементов управления Internet Explorer – ActiveX.
Вредоносная программа может автоматически устанавливаться на ваш ПК, смартфон или планшет без нажатия на веб-ссылку.
Другой вариант установки – в виде всплывающего окна

Меры защиты

1. Игнорируйте все неожиданные всплывающие окна, предупреждения о новых вирусах или предложения загрузить бесплатное ПО
2. Никогда не нажимайте кнопку «Загрузить» и всегда осторожно закрывайте объявления
3. Используйте блокировщики всплывающих окон и фильтры URL-адресов
4. Удаляйте ненужные программы и приложения
5. Сообщайте в ИТ-отдел об инцидентах