МИНЦИФРА
Республики Татарстан

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

МИНЦИФРА
Республики Татарстан

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)

МИНЦИФРА
Республики Татарстан

Виды информации

Информация ограниченного доступа

- Государственная тайна
- Конфиденциальная информация

Общедоступная информация

- Информация, доступ к которой не может быть ограничен
- Иная информация

Типы конфиденциальной информации

МИНЦИФРА
Республики Татарстан

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

МИНЦИФРА
Республики Татарстан

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

МИНЦИФРА
Республики Татарстан

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

МИНЦИФРА
Республики Татарстан

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)

МИНЦИФРА
Республики Татарстан

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

МИНЦИФРА
Республики Татарстан

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

МИНЦИФРА
Республики Татарстан

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

МИНЦИФРА
Республики Татарстан

Цифры года

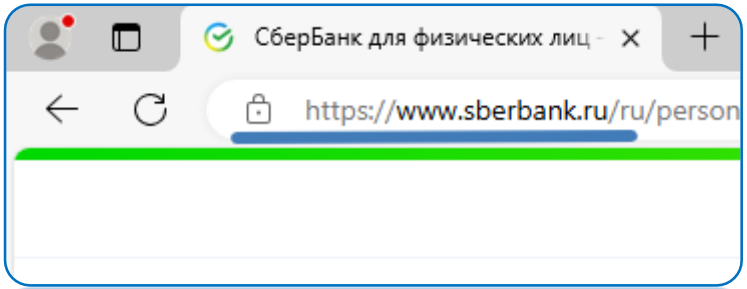
По данным представленным от Лаборатории Касперского:

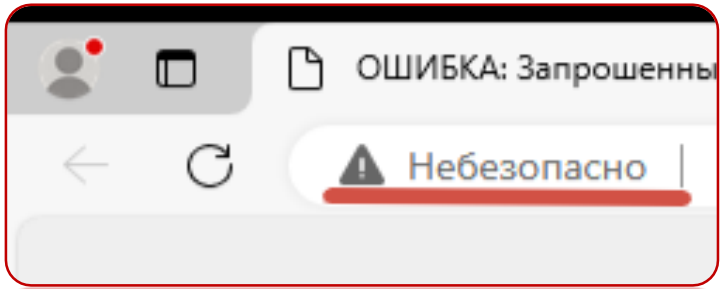
- 45,60% электронных писем по всему миру и 46,59% писем в Рунете были спамом
- 31,45% всех спамовых писем были отправлены из России
- почтовый антивирус Касперского заблокировал 135 980 457 вредоносных почтовых вложений

МИНЦИФРА
Республики Татарстан

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

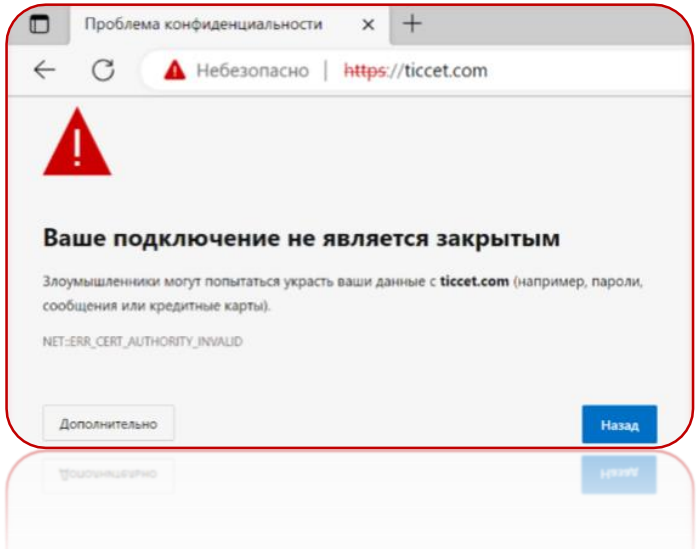




МИНЦИФРА
Республики Татарстан

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



МИНЦИФРА
Республики Татарстан

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

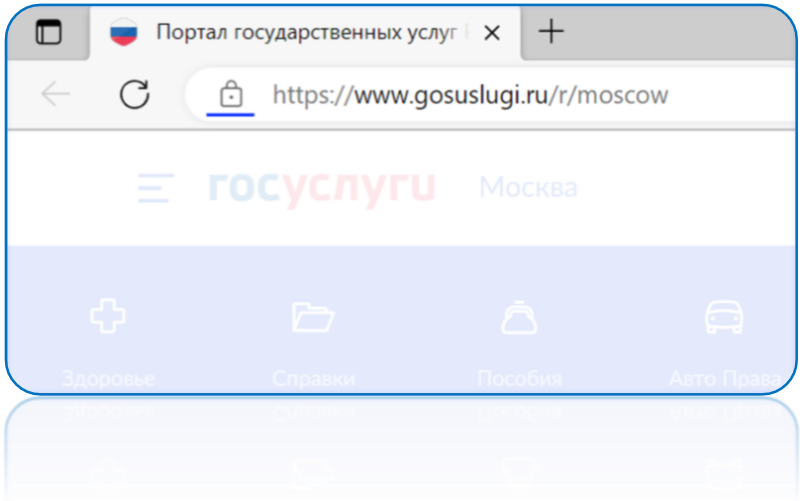
Насторожить должны

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

МИНЦИФРА
Республики Татарстан

4. Проверяйте наличие SSL-сертификата

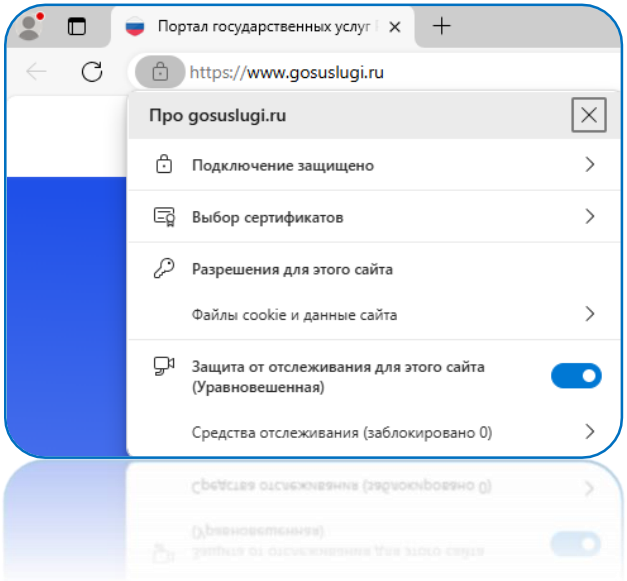
Если в строке перед адресом есть значок замочка, а перед именем сайта указан протокол HTTPS, значит, сайт имеет SSL-сертификат, а соединение между сервером и браузером пользователя зашифровано и безопасно



МИНЦИФРА
Республики Татарстан

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



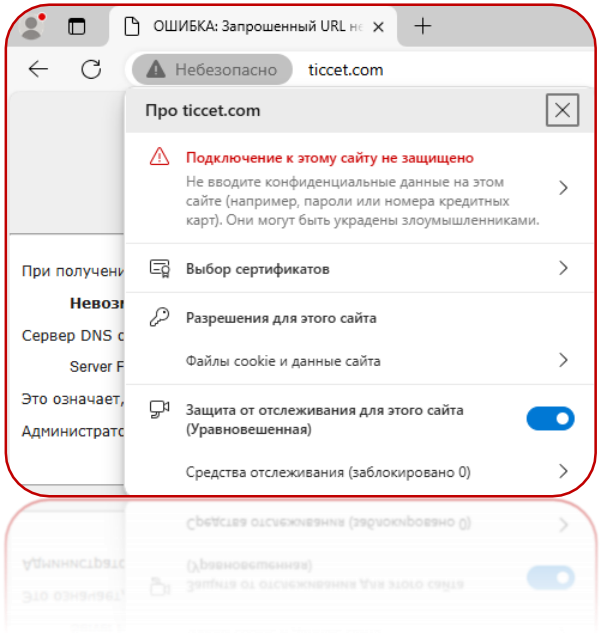
МИНЦИФРА
Республики Татарстан

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.

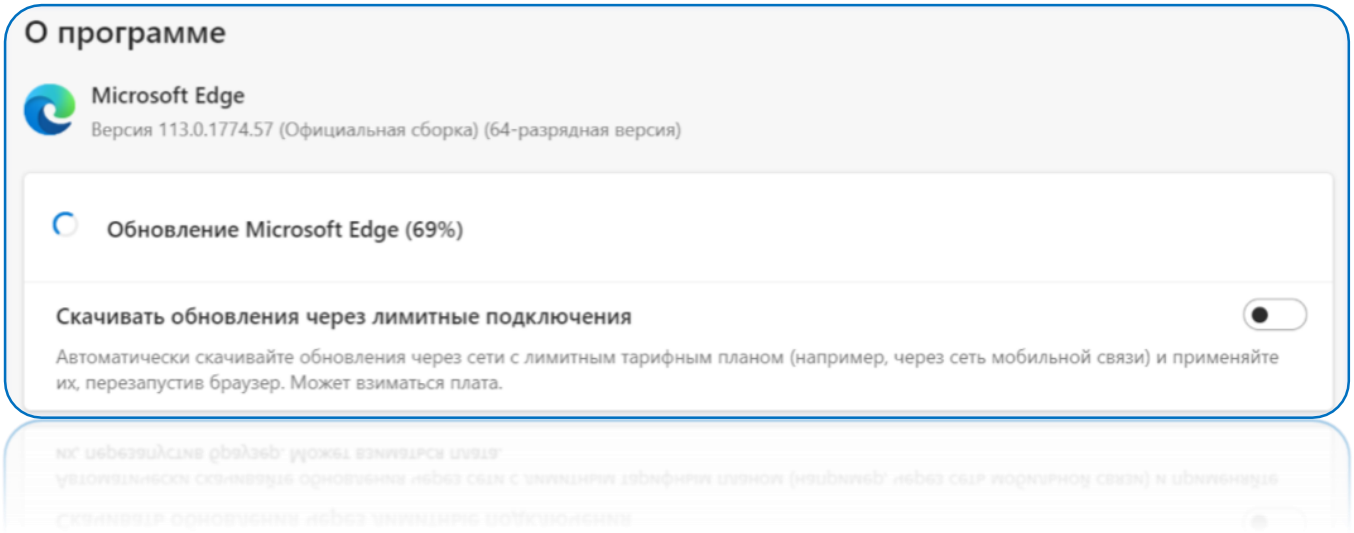
Сайты без SSL-сертификата передают и принимают данные в открытом виде, поэтому их легче перехватить и подменить



МИНЦИФРА
Республики Татарстан

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



МИНЦИФРА
Республики Татарстан

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

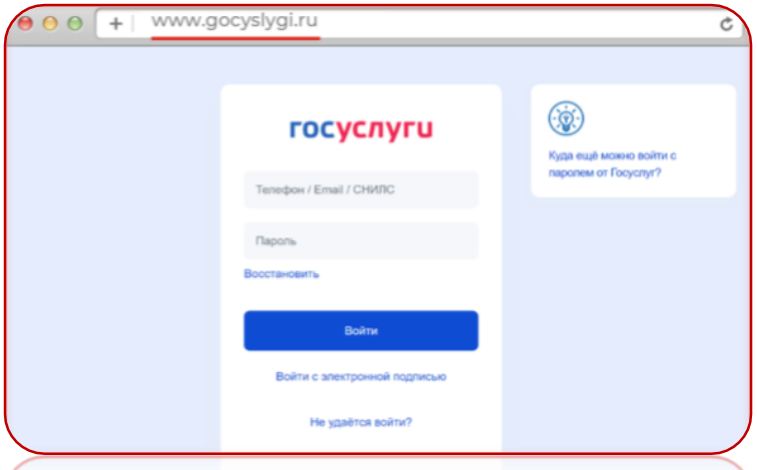
Чтобы пользователи вводили на сайтах свои данные, мошенники правдоподобно подделывают эти сайты

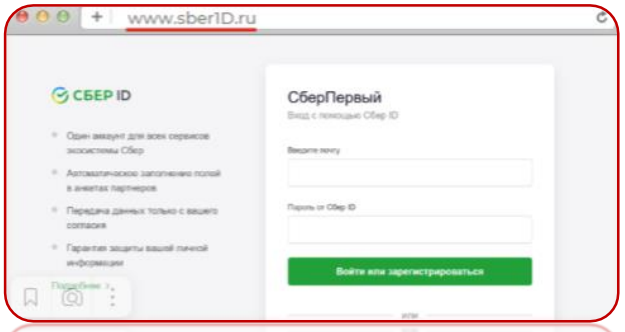
Внимательно изучите сайт, прежде чем вводить на нем свои данные, и не переходите по подозрительным ссылкам!

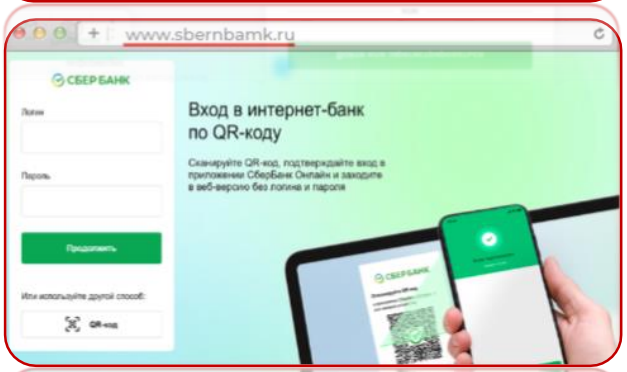
МИНЦИФРА
Республики Татарстан

Примеры фишинговых сайтов

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





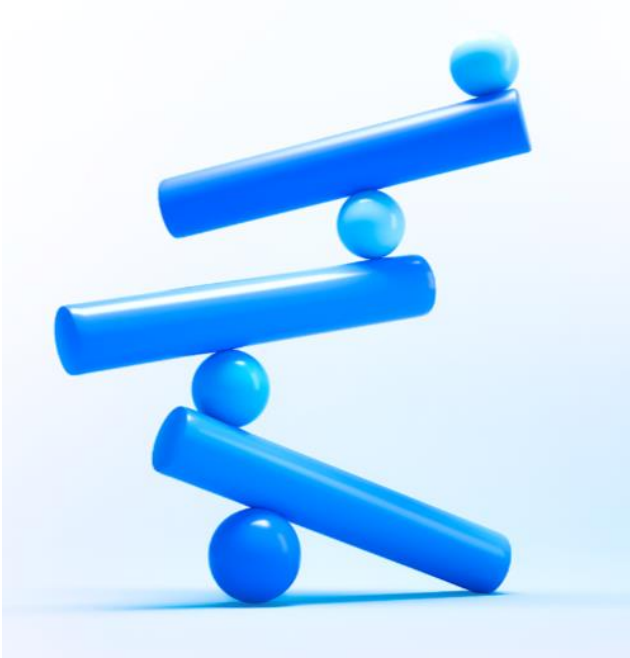


МИНЦИФРА
Республики Татарстан

7. Используйте сложные пароли

Чем длиннее пароль,
тем сложнее его взломать

Для запоминания сложных
паролей используйте
менеджер паролей или
собственную память



МИНЦИФРА
Республики Татарстан

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

МИНЦИФРА
Республики Татарстан

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

МИНЦИФРА
Республики Татарстан

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

МИНЦИФРА
Республики Татарстан

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

МИНЦИФРА
Республики Татарстан

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