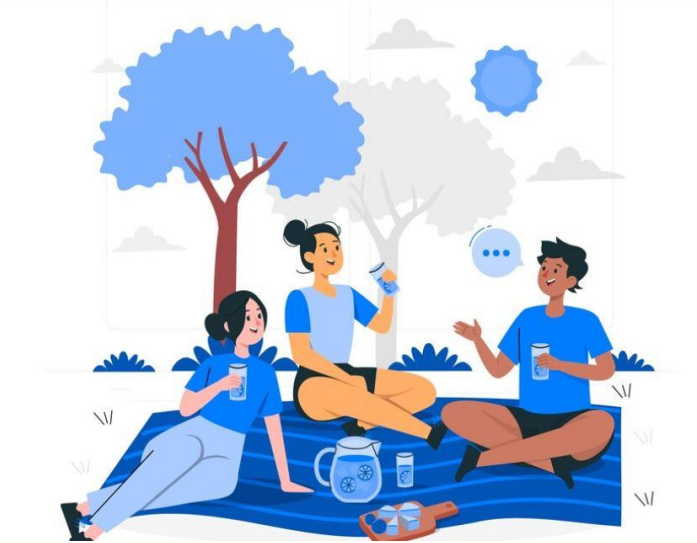
ЦИФРОВАЯ БЕЗОПАСНОСТЬ В СОВРЕМЕННОМ МИРЕ

Как провести курсы по информационной безопасности с пользователями зрелого возраста

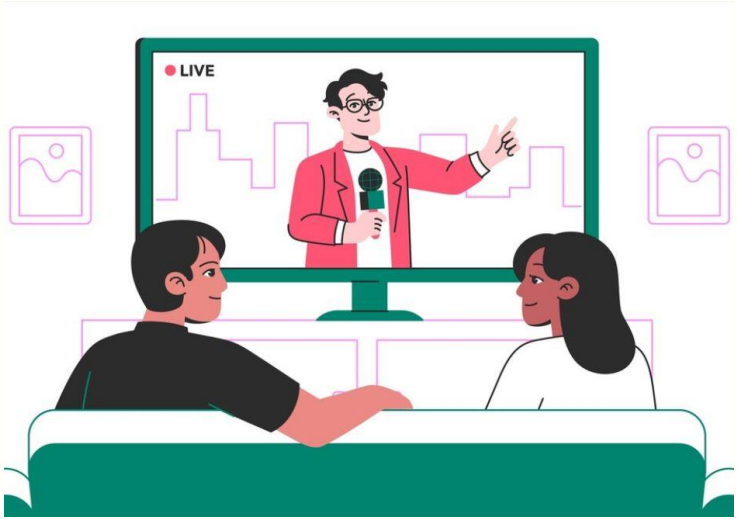
Основные моменты, которые важно учитывать

СРЕДА ОБЩЕНИЯ ЧЕЛОВЕКА

ФИЗИЧЕСКИЙ МИР



ВИРТУАЛЬНЫЙ МИР
(цифровое пространство)



УРОВНИ ЦИФРОВОГО ПРОСТРАНСТВА



ИНФРАСТРУКТУРНЫЙ

- ✓ КОМПЬЮТЕРЫ
- ✓ ТЕРМИНАЛЫ
- ✓ МОБИЛЬНЫЕ УСТРОЙСТВА

УРОВНИ ЦИФРОВОГО ПРОСТРАНСТВА



ЛОГИЧЕСКИЙ

- ✓ ОПЕРАЦИОННЫЕ СИСТЕМЫ
- ✓ ПРИЛОЖЕНИЯ
- ✓ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

УРОВНИ ЦИФРОВОГО ПРОСТРАНСТВА



ЦИФРОВАЯ ЖИЗНЬ

- ✓ СОЦИАЛЬНЫЕ СЕТИ
- ✓ БАНКОВСКИЕ ОПЕРАЦИИ
- ✓ ГОС. УСЛУГИ

Указ Президента РФ от 02.07.2021 N 400
"О Стратегии национальной безопасности Российской Федерации"



Указ Президента РФ от 02.07.2021 N 400 "О Стратегии национальной безопасности Российской Федерации"

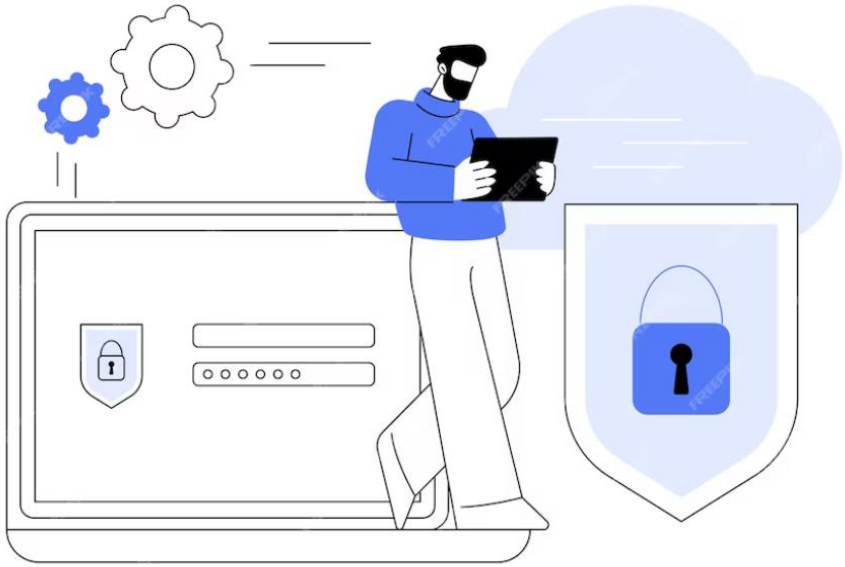
- Указ
- Стратегия национальной безопасности Российской Федерации
  - I. Общие положения
  - II. Россия в современном мире: тенденции и возможности
  - III. Национальные интересы Российской Федерации и стратегические национальные приоритеты
  - IV. Обеспечение национальной безопасности
    - Сбережение народа России и развитие человеческого потенциала
    - Оборона страны
    - Государственная и общественная безопасность
    - Информационная безопасность
    - Экономическая безопасность
    - Научно-технологическое развитие
    - Экологическая безопасность и рациональное природопользование
    - Защита традиционных Российских духовно-нравственных ценностей, культуры и исторической памяти
    - Стратегическая стабильность и взаимовыгодное международное сотрудничество
  - V. Организационные основы и механизмы реализации настоящей Стратегии

ЦИФРОВАЯ БЕЗОПАСНОСТЬ

КИБЕРБЕЗОПАСНОСТЬ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

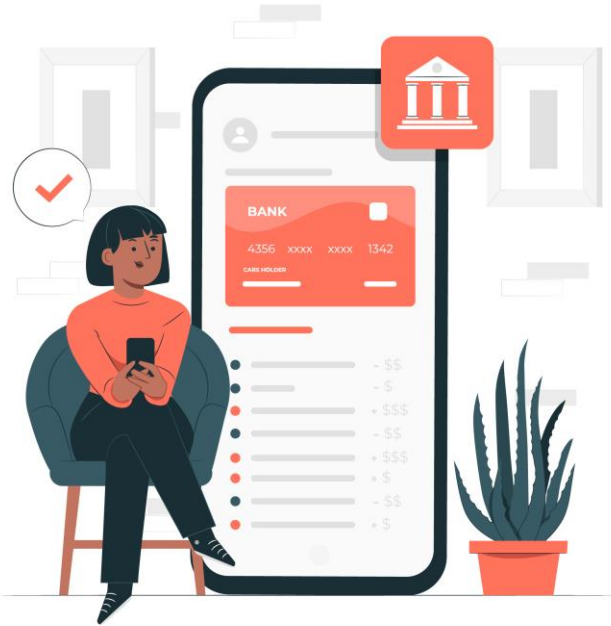
Информационная безопасность



- ✓ Виды мошенничества в сети
- ✓ Вредоносные программы и вирусы
- ✓ Антивирусные программы
- ✓ Меры предоторожности в сети
- ✓ Защита от взлома аккаунта

Интернет-платежи

УГРОЗЫ ПРИ ПРОВЕДЕНИИ: ОСНОВНЫЕ АТАКИ



- ✓ Технологические атаки – подмена сайтов, на которые заходит пользователь
- ✓ Социальная инженерия, фишинг (в эл. Почте, в мессенджерах, на сайтах)
- ✓ Заражение СМС-троянцами – перехват данных пользователя

Интернет-платежи

ЧТО ОТВЕЧАЕТ ЗА БЕЗОПАСНОСТЬ ПЛАТЕЖЕЙ?

Проверка сертификатов

В защищенном режиме Браузер включает строгий режим проверки сертификатов HTTPS. Защищенный режим не включается, если:

- возникли проблемы с сертификатом, например, сертификат банка устарел, недействителен или не является доверенным;
- используется неизвестный сертификат, установленный в операционную систему программой или администратором сети;
- используется сертификат, установленный специальным ПО.

Внимание

Если защищенный режим не включился, совершать электронные платежи небезопасно и мы рекомендуем этого не делать.

- ✓ Протокол SSL (безопасная передача зашифрованной информации от пользователя к серверу)
- ✓ Стандарты безопасности карт, разработанные международными платежными системами
- ✓ Проверка личности путем отправки SMS с кодом (технология 3D Secure)
- ✓ Противомошеннические системы в банках

Интернет-платежи

КАК ЗАЩИТИТЬ СВОИ ДЕНЬГИ ПРИ СОВЕРШЕНИИ ПЕРЕВОДОВ?

- ✓ Подключите интернет-банк и СМС-оповещение
- ✓ Используйте только защищённые сайты (https:// - сертификаты НУЦ (Национальный удостоверяющий центр) Минцифры России)
- ✓ Используйте авторизацию платежа по СМС с кодом

Интернет-платежи

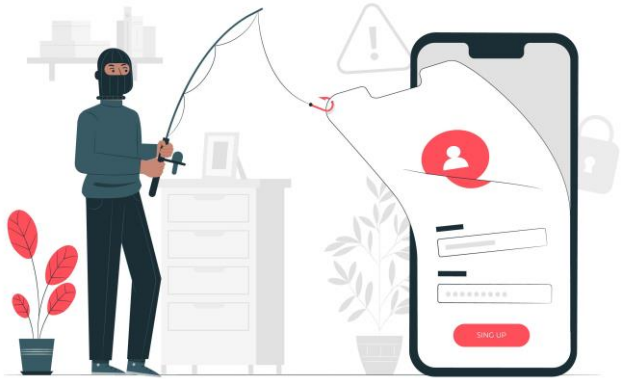
ДОПОЛНИТЕЛЬНЫЕ СОВЕТЫ

- ✓ Заведите отдельную банковскую карту для интерент-платежей
- ✓ Используйте надёжные пароли и не используйте один и тот же пароль для всех своих аккаунтов
- ✓ Не используйте для оплаты карты с большим кредитным лимитом
- ✓ Никогда не сообщайте данные своей банковской карты другим людям
- ✓ Совершайте покупки с устройств, на которых установлена антивирусная защита

Фишинг в соцсетях, мессенджерах, эл.почте

- ✓ Мошенник создаёт копию сайта (банка, соцсети и т.д.)
- ✓ Пользователь получает ссылку на поддельный сайт, например прочитать важное сообщение
- ✓ Идёт по ссылке на фишинговый сайт и вводит свои данные для входа в систему (аккаунт)
- ✓ Введённые данные отправляются злоумышленнику

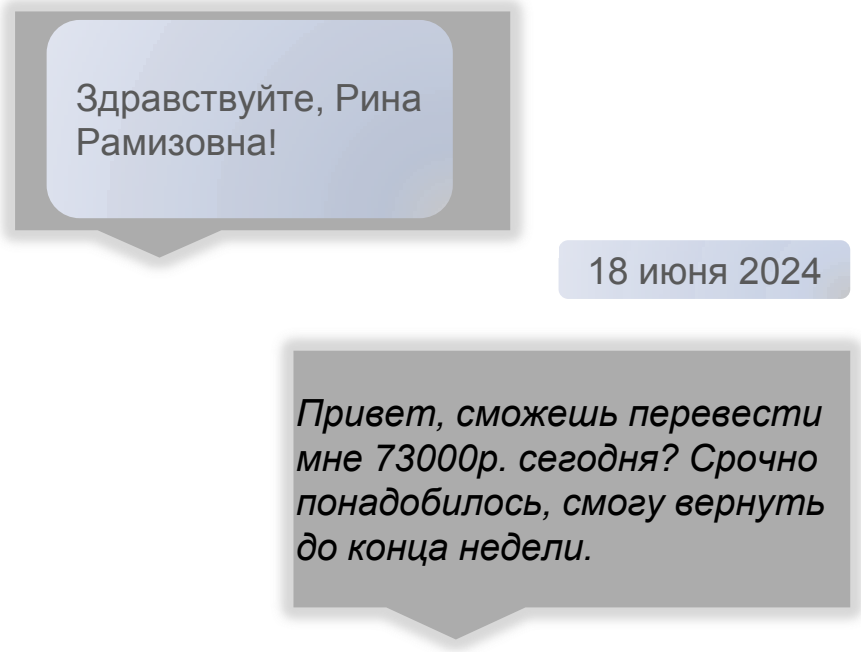
ПРИМЕРНЫЙ СЦЕНАРИЙ ФИШИНГА



Фишинг в соцсетях, мессенджерах, эл.почте

- ✓ Просьба помочь жертвам катаклизмов
- ✓ Выигрыш в лотерею
- ✓ Предложение выиграть новый телефон
- ✓ Розыгрыш бесплатных авиабилетов

АКТУАЛЬНЫЕ МОШЕННИЧЕСКИЕ СХЕМЫ



Фишинг в соцсетях, мессенджерах, эл.почте

- ✓ Кража данных от банковских счетов, похищение денег
- ✓ Кража аккаунта в соцсети или электронной почты для рассылки спама
- ✓ Заражение компьютера пользователя, для внедрения различных программ
- ✓ Шантаж, подписка пользователей на платные услуги (в т.ч. через СМС)

ЦЕЛИ ФИШЕРОВ



Фишинг в соцсетях, мессенджерах, эл.почте

- ✓ Вам предлагают принять выгодное решение в сжатые сроки
- ✓ Наличие ссылок по нажатию на которые предлагается что-то скачать
- ✓ В содержании сообщения (письма) много грамматических и стилистических ошибок
- ✓ Вас просят прислать ваши личные данные, пароль, ПИН-код, код из СМС и т.д.

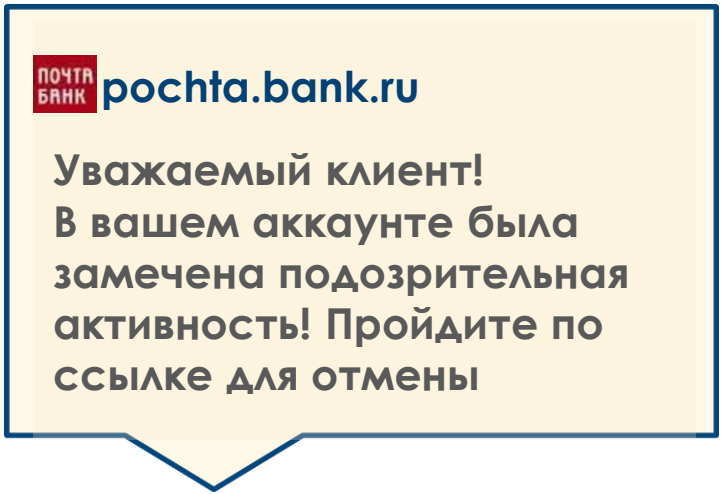
ПРИМЕРЫ ФИШЕНГОВЫХ СООБЩЕНИЙ



Фишинг в почте, соцсетях, мессенджерах

- ✓ Письмо приходит со странного домена (@yasdow.com)
- ✓ В письме от гос. организации отсутствует цифровая подпись и к вам обращаются «Уважаемый клиент», но не по имени
- ✓ На письмо отреагировала антивирусная программа
- ✓ В письме есть вложения в формате .exe, .vbs, .scr

ПРИМЕРЫ ФИШЕНГОВЫХ ПИСЕМ



Правила безопасности в сети

- ✓ Своевременно обновляйте свой браузер, установите антивирусное ПО
- ✓ Используйте двухфакторную аутентификацию (например через СМС)
- ✓ Не делайте вход в онлайн-банки и другие свои аккаунты через открытые Wi-Fi в общественных местах или на улице
- ✓ Внимательно проверяйте ссылки, по которым переходите. Вводите адрес веб-сайтов вручную

КАК НЕ СТАТЬ ЖЕРТВОЙ ФИШИНГА



Дезинформация в сети

- ✓ Вымышленные новости
- ✓ Фотографии, обработанные в фотошопе
- ✓ Слухи и домыслы
- ✓ Вымышленные аккаунты в социальных сетях



Культура безопасного поведения в цифровой среде

- ✓ **ОСОЗНАННОСТЬ** – всё, что вы создаёте в цифровом пространстве, может быть зафиксировано и использовано другими
- ✓ **КРИТИЧЕСКОЕ МЫШЛЕНИЕ** – проверьте информацию в разных источниках, оценивайте надёжность источника. Обращайте внимание на название, дату и время , а также автора публикации
- ✓ **ОТВЕТСТВЕННОСТЬ** – будьте ответственны за свои транслируемые слова и действия
- ✓ **УВАЖЕНИЕ** – не распространяйте ложную (непроверенную) информацию, уважайте других пользователей

ОСНОВЫ ЦИФРОВОЙ ГРАМОТНОСТИ И ИНФОРМАЦИОННОЙ КУЛЬТУРЫ

- Компьютерная грамотность: начальный курс
- Основы информационной грамотности
- Социально-значимая информация в сети Интернет

Компьютерная грамотность: начальный курс

Устройство компьютера

Системный блок, монитор, клавиатура, мышь



Программы. Рабочий стол

Главное меню. Панель задач. Настройки. Структура





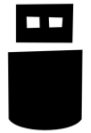
Работа в текстовом редакторе

Панель инструментов. Редактирование, сохранение, распечатка текста

Организация хранения данных

Файлы, папки. Флеш-диски. Управление окнами





Основы информационной грамотности



- ✓ Введение в Интернет
- ✓ Браузер. Основы поиска
- ✓ Безопасная работа в сети
- ✓ Электронная почта
- ✓ Сохранение информации из Интернет
- ✓ Загрузки. Панель закладок

Социально-значимая информация в сети интернет

Портал Госуслуги

Регистрация. Личный кабинет. Электронные услуги

Здравоохранение

Запись к врачу. Сервисы по поиску лекарств.

Госсайты. ЖКХ

Сайты федеральных органов власти. Информационные порталы. Сервисы расчёта коммунальных платежей.

Интернет для туризма

Готовые туры. Маршруты путешествий. Бронирование номеров в отелях. Покупка билетов. Форумы

Культурно-значимые и досуговые ресурсы

Онлайн-лектории. Виртуальные музеи. Электронные библиотеки. Видеосервисы

Освоить навыки информационной безопасности доступно всем!

ИЗУЧЕНИЕ

ПРАКТИКА

ПРИМЕНЕНИЕ

Спасибо за внимание!

Закирова Рина Рамизовна
Заведующая отделом электронных ресурсов

СОУНБ им. В.Г. Белинского

+7 (343) 304-60-20, доб. 320

inform@uraic.ru