

КИБЕР БАЗА

как защитить себя
и свое цифровое пространство



Рост киберугроз в мире



2,2 млн

киберпреступников

445 млн

киберпреступлений

\$1,6 млн

стоимость устранения
последствий программ-
вымогателей

3,5 млн

человек дефицит
кадров в сфере
кибербезопасности

2,1 млн

фишинговых
сайтов

\$4,4 млн

стоимость утечки
данных

Что нужно хакерам?

КРАЖА ЛИЧНОСТИ ДЕНЕГ

в 70%

случаев люди сами переводят деньги или предоставляют свои платежные данные

<1 мин.

необходимо, чтобы получить данные паспорта и личную почту по фото посадочного талона



Угрозы в киберпространстве



Взлом облачных хранилищ

Все ваши фоточки из облачных хранилищ (iCloud, Google Disk, Облако Mail.ru и другие) в руках шантажистов

Фейковые инвестиции

«Зачем тебе вклад под 5% годовых? 200% год при минимальном риске на супердоходном проекте!»

Вредоносное ПО

От надоедливых рекламных баннеров и вымогательства до полного «сноса» ОС и удаления данных жесткого диска

Удаленная работа

«30 000 рублей в день! Все, что тебе нужно – пара часов в день и ноутбук. Всем обучим сами»

Социальная инженерия

«Здравствуйте, я из отдела МВД, переведите деньги на защищенный счет»

Фишинг

Электронные письма или СМС-сообщения, побуждающие переходить на поддельные сайты

Как выглядит вирусная угроза



Произвольно запускаются программы, удаляются файлы и папки, искажается их содержимое

Ваши друзья получают от вас сообщения, которые вы не отправляли, наблюдаются частые зависания и сбои системы

На экране появляются подозрительные сообщения, рекламные окна

Основные источники вирусного заражения



на компьютерах

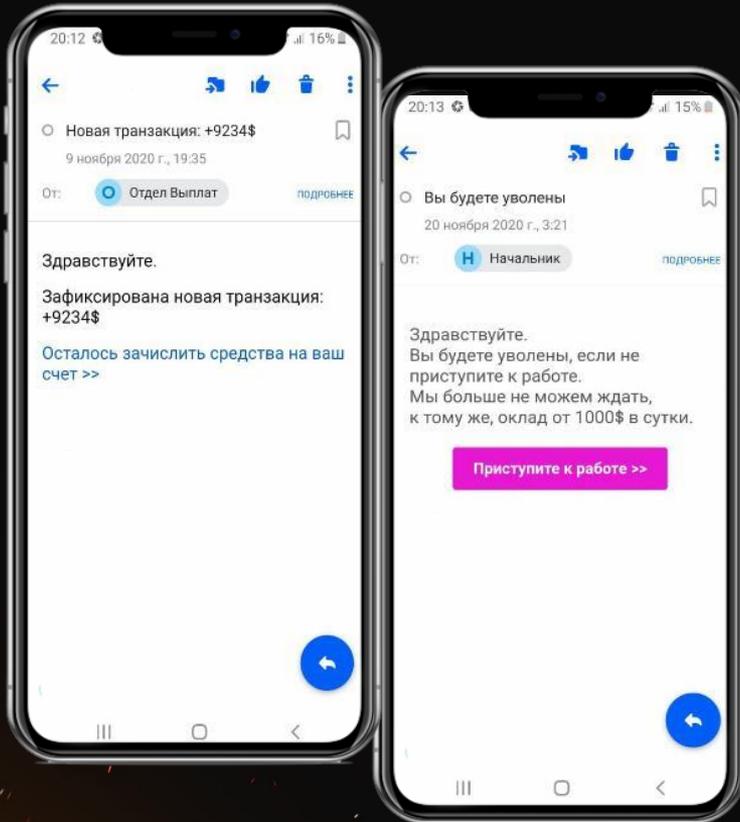
- Переход по ссылкам и открытие вложенных файлов в письмах от неизвестных отправителей
- Скачивание и установка нелегального ПО
- Подключение неизвестных съемных носителей



на мобильных устройствах

- Скачивание и установка приложений из неавторизованных источников
- Переход по ссылкам из сообщений в соцсетях, мессенджерах и почте
- Физический доступ к вашему устройству

Что такое фишинг



Фишинг

Вид интернет-мошенничества с использованием рассылок вредоносных электронных писем с целью получения доступа к конфиденциальным данным пользователей (логинам, паролям, данным банковской карты и т.д.) или денежным средствам



Телефонное мошенничество



«С вашего счета хотят украсть деньги...»

«Продиктуйте код для отмены мошеннической операции...»

«На вас оформили кредит в другом городе...»

Мошенники хорошо подготовлены и обучены психологическим трюкам, чтобы запутать потенциальную жертву и заставить ее совершить необдуманный поступок

хакеры

мошенники



манипуляторы

маньяки

хейтеры

драгдилеры

Думаешь, что тебя
это не касается?

Манипуляторы

Распространяют фейковую
информацию и новости

Зовут тебя на баррикады

Заставляют тебя делать
то, что тебе не нужно

Думай, а свои ли
желания ты выполняешь!



Хейтеры

- В соцсети создается подставной профиль (например, девушки)
- С этого аккаунта пишутся оскорбления / провокации другим пользователям
- Жертвы буллинга начинают интересоваться тем, кто шлет им гадости и переходят на страницу «обидчицы»
- Не найдя никакой полезной информации, кликают по единственной размещенной на странице ссылке, которая ведет на фишинговый сайт
- Фишинговый сайт копирует страницу входа на другую популярную соцсеть

Если введете свой логин и пароль, мошенник получит контроль над вашим аккаунтом



Любое наше действие в сети оставляет цифровой след

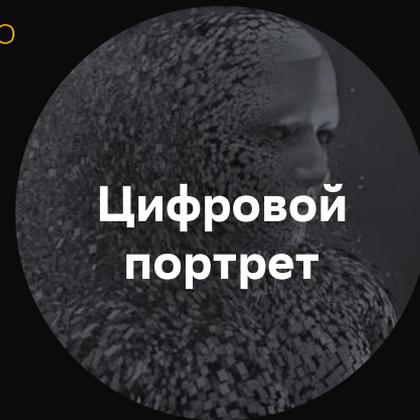
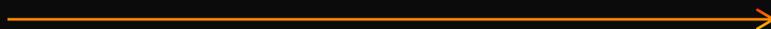


Цифровой след

регистрация на сайтах

фото и видео

лайки в соцсетях



Цифровой портрет

посты и репосты

комментарии к постам



**Кнопки «Удалить» в интернете нет
Полной анонимности не существует
Информация, попавшая в сеть, остается там навсегда**

Политика конфиденциальности



При размещении данных на сайте ты фактически теряешь контроль за их использованием и распространением

В пользовательских соглашениях есть пункты, которые гласят:



«Администрация Сайта считает, что Пользователь осознает, что информация на Сайте, размещаемая Пользователем о себе, может становиться доступной для других Пользователей Сайта и пользователей Интернета, может быть скопирована и распространена такими пользователями...»



«Мы делимся вашими данными с нашими сторонними поставщиками услуг, которых мы используем, чтобы предоставлять вам доступ к Платформе. Мы также предоставляем вашу информацию нашим деловым партнерам, рекламодателям, операторам аналитических и поисковых систем...»

VPN

Ваш реальный IP-адрес подменяется адресом VPN-сервера — местоположение и личность замаскированы, так как запрашиваемый сайт видит только адрес, который дал VPN

Для чего используется

- шифрование трафика защита ценных данных от перехвата
- доступ к сайтам и мессенджерам
- смена геолокации в целях шопинга
- анонимность
- безопасное соединение между домом и офисом

Чем опасны VPN-сервисы

- недобросовестность сервисов
- собирают информацию о вас для перепродажи
- плохо защищают данные
- увеличивают количество рекламы, подмешивая ее в трафик
- вредоносные программы могут выдавать себя за VPN-приложения



Как защитить себя в киберпространстве



Включи голову

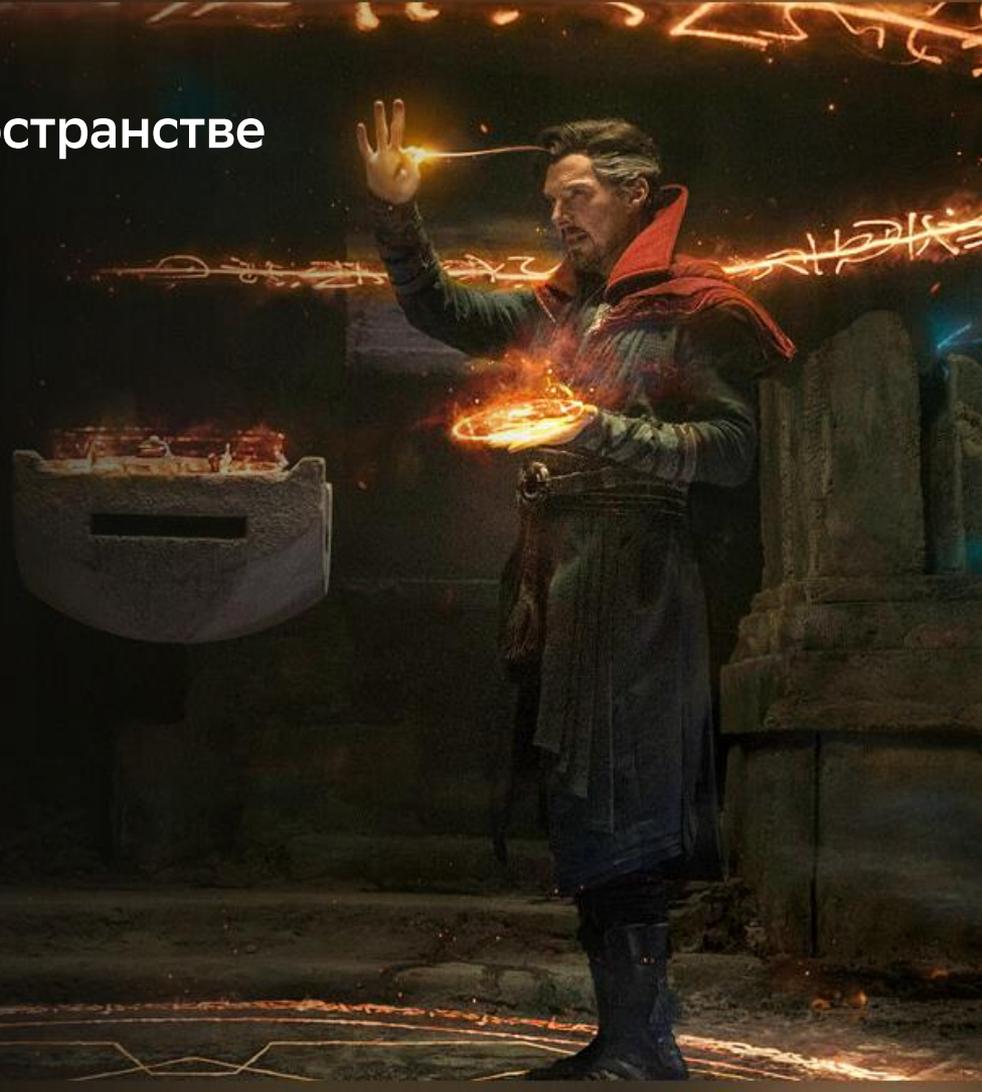
Защищай свои устройства

Используй сложные пароли

Настрой безопасность данных

Соблюдай правила общения

Будь финансово грамотным



Защитай свои устройства и аккаунты



Сложные пароли



Двухфакторная
идентификация



Официальный софт



Осторожно с облаками



Регулярные обновления

Используй сложные пароли



60%

пользователей используют одинаковые или похожие пароли на нескольких учетных записях



Сколько времени нужно, чтобы взломать пароль:

| Кол-во знаков | Только цифры | Строчные буквы | ПРОПИСНЫЕ строчные буквы | Цифры ПРОПИСНЫЕ строчные буквы | Цифры ПРОПИСНЫЕ строчные буквы символы |
|---------------|--------------|----------------|--------------------------|--------------------------------|--|
| 8 | МГНОВЕННО | 5 сек. | 22 мин. | 1 час | 8 часов |
| 9 | МГНОВЕННО | 2 мин. | 19 ч. | 3 дня | 3 недели |
| 10 | МГНОВЕННО | 58 мин. | 1 месяц | 7 мес | 5 лет |
| 11 | 2 сек. | 1 день | 5 лет | 41 год | 400 лет |
| 12 | 25 сек. | 3 недели | 300 лет | 2 тыс. лет | 34 тыс. лет |

Обязательно должен быть сложный пароль



на электронной почте



в интернет-банке



в соцсетях и мессенджерах

Как распознать фишинг



1. Обращайте внимание на домен. Мошенники обычно используют общедоступные почтовые домены gmail.com, mail.ru и т.п., или покупают домены, похожие на официальные имена компаний, чтобы ввести получателя в заблуждение
2. Вас должно насторожить, если тема, контент письма или название файлов побуждают вас к немедленному действию
3. Обращайте внимание на обращение и подпись. Если они являются безличными, или есть признак автоподстановки в обращении, то высока вероятность фишинга. Контакты могут быть недостоверные, проверьте их на официальном сайте компании.
4. Не переходите по ссылкам, не кликайте на подозрительные объекты. Наведите курсор мыши на подозрительную ссылку/объект и вы увидите, куда она ведёт на самом деле. Сравните её с официальным сайтом компании.
5. Будьте осторожны с вложениями, открывайте только те, которые ждали
6. Не вводите свои данные, логин и пароль на подозрительных сайтах или в какие-либо анкетные формы
7. Не отвечайте на подозрительные письма

Наши сервисы помогут себя защитить



Кибрарий

Библиотека знаний по кибербезопасности



«Не дайте себя обмануть»

Обучающий раздел в Сбербанк Онлайн



Осторожно, мошенники!

Канал в Сбербанк Онлайн об актуальных схемах мошенничества



Ничего личного

Канал в Сбербанк Онлайн о защите персональных данных



Будьте бдительны!