АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ
«ЦЕНТР ТЕХНОЛОГИЙ ЭЛЕКТРОННОЙ ДЕМОКРАТИИ»

ЭЛЕКТРОННОЕ УЧЕБНОЕ ПОСОБИЕ

"ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ"

Автор-составитель: Маслова Н.Р.,

руководитель проекта, к.т.н

Ханты-Мансийск 2022

Электронное учебное пособие «Основы кибербезопасности» разработано в рамках проекта «Цифровая трансформация на службе граждан» для тьюторов и слушателей одноименного курса.

Автор-составитель Маслова Наталья Рудегеровна, руководитель проектов «Цифровая экономика для гражданского общества» и «Цифровая трансформация на службе граждан», кандидат технических наук. Учебное пособие разработано как дополнительный материал к курсу ««Цифровая трансформация на службе граждан» с учетом национальной цели «Цифровая трансформация», утвержденной Указом Президента Российской Федерации от 21 июля 2020 года № 474 «О национальных целях развития Российской Федерации на период до 2030 года» и нормативных правовых актов по Стратегическим направлениям в области цифровой трансформации государственного управления, социальной сферы, образования, науки и высшего образования, здравоохранения и др.

Раздел курса по изучению основ кибербезопасности, посвящен защите данных, представленных в цифровой форме и направлен на получение знаний о киберугрозах и методах защиты от них, формирование практических навыков по использованию средств противодействия киберугрозам.

Учебное пособие рекомендуется использовать тьюторам как дополнительный материал при подготовке к проведению занятий по Учебно-методическому пособию «Цифровая трансформация на службе граждан» (далее УМП), Блок 3. Учебное пособие предназначено для размещения в личном кабинете тьютора.

Слушателям курса «Цифровая трансформация на службе граждан» следует использовать материалы учебного пособия при самостоятельном изучении разделов Блока 3 «Основы кибербезопасности» в УМП.

Материалы Электронного учебного пособия «Основы кибербезопасности» будут также полезны слушателям при подготовке к практическим занятиям и к тесту по данному курсу.

ИСТОЧНИКИ:

https://iot.ru/wiki/kiberbezopasnost
https://www.gosuslugi.ru
https://www.sberbank.ru
https://www.kaspersky.ru/resource-center
http://www.tadviser.ru

СОДЕРЖАНИЕ

ВВЕДЕНИЕ
1. ЧТО ТАКОЕ КИБЕРБЕЗОПАСНОСТЬ?
2. БЕЗОПАСНОСТЬ ПРИ РАБОТЕ С ПОРТАЛОМ ГОСУСЛУГ
3. РЕКОМЕНДАЦИИ КИБЕРБЕЗОПАСНОСТИ СБЕРБАНКА
4. РЕКОМЕНДАЦИИ КИБЕРБЕЗОПАСНОСТИ «ЛАБОРАТОРИИ КАСПЕРСКОГО»
5. МОШЕННИЧЕСТВО С БАНКОВСКИМИ КАРТАМИ. ПРИМЕРЫ КИБЕРБЕЗОПАСНОСТИ ОТ TADVISER
6. ДОПОЛНЕНИЯ (2021 – 2022 г.г.)

ВВЕДЕНИЕ

Благодаря цифровой экономике повышается эффективность, скорость взаимодействия всех отраслей за счет использования современных средств связи и информационных технологий. Рабочая деятельность, личная и социальная жизнь все активнее переходит в цифровое пространство. Но цифровая трансформация несет и определенные риски.

Целью кибербезопасности является обеспечение трех наиболее важных принципов: конфиденциальности, целостности и доступности данных.

Информация и данные должны быть постоянно легко доступны и в то же время надежно защищены от неправомерного использования. Искажение или фальсификация, уничтожение или разглашение определенной части информации, также, как и нарушение процессов её обработки и передачи, наносят серьезный урон субъектам информационного взаимодействия.

Таким образом, крайне остро встаёт вопрос обеспечения кибербезопасности как различных государственных и муниципальных структур, коммерческих и некоммерческих организаций, так и цифровых устройств и персональных данных физических лиц.

Важно иметь компетенции по способности оценивать уровень киберзащищенности данных, идентифицировать угрозы кибербезопасности, обеспечить кибербезопасность персональных данных и рабочих процессов.

История создания и развития кибербезопасности.

https://iot.ru/wiki/kiberbezopasnost

На ранних стадиях развития сетей связи вопросы безопасности не были главными из-за небольшого количества пользователей и наличия в основном локальных сетей, в которых подразумевается доверие всех пользователей друг другу. С развитием технологий и разрастанием сетей связи выросло и значение обеспечения безопасности.

История кибербезопасности начинается с появления первых атак на компьютеры. В 1989 году Робертом Моррисом был создан первый компьютерный червь – самораспространяющийся вирус. Конечно, атаки и вирусы существовали и до этого времени, но именно червь Морриса был первой масштабной и широко распространенной DoS атакой (англ. Denial of Service – «отказ в обслуживании») в сети ARPANET – предшественник Интернета.

В 1990-х годах в США был создан Консорциум по исследованиям в области информационной безопасности, в рамках которого разработали предложение по Международной конвенции по борьбе с киберпреступностью и терроризмом. В сентябре 1997 года был опубликован документ RFC 2196, который представлял собой руководство по разработке политики в области компьютерной безопасности в рамках интернет-сообщества. В 2014 году Европейским институтом стандартизации электросвязи (ETSI) был создан технический комитет Cyber Security, отвечающий за стандартизацию кибербезопасности на международном уровне.

В настоящее время кибербезопасность приобретает все большее значение в связи с растущим влиянием компьютерных систем и Интернета на все сферы жизни, развитием беспроводных сетей (например, на базе Bluetooth и Wi-Fi), а также ростом «умных» устройств, смартфонов, телевизоров как части Интернета вещей.

Основу кибербезопасности составляют три процесса:

- предотвращение угрозы;
- обнаружение угрозы;
- реагирование.

Наша задача дать общие представления о безопасности в информационном обществе и на этой основе сформировать понимание технологий информационной безопасности и умения применять правила кибербезопасности во всех сферах деятельности.

1. ЧТО ТАКОЕ КИБЕРБЕЗОПАСНОСТЬ?

Кибербезопасность – это реализация мер по защите систем, сетей и программных приложений от цифровых атак. Такие атаки обычно направлены на получение доступа к конфиденциальной информации, ее изменение и уничтожение, на вымогательство у пользователей денег или на нарушение нормальной работы компаний.

Сегодня внедрение эффективных мер кибербезопасности особенно трудно, поскольку устройств стало больше, чем людей, а хакеры применяют все более изощренные методы атак.

Более подробно – в следующих разделах учебного пособия и в Блоке 3. Основы кибербезопасности УМП.

Указ Президента РФ от 1 мая 2022 года № 250 “О дополнительных мерах по обеспечению информационной безопасности” затронул около 500 тысяч организаций. Согласно этому документу, компаниям предстоит назначить заместителя генерального директора по ИБ, создать отдел ИБ и выстроить процессы кибербезопасности по новому регламенту.

2. БЕЗОПАСНОСТЬ ПРИ РАБОТЕ С ПОРТАЛОМ ГОСУСЛУГ https://www.gosuslugi.ru

О защите персональных данных

Информационная безопасность является одной из важных компонент предоставления государственных услуг в электронном виде. При создании и доработке портала госуслуг регулярно проводится работа по анализу возможных угроз, на основе которых сформированы требования по защите информации при использовании портала. В системе безопасности портала госуслуг используется обширный набор механизмов безопасности: межсетевые экраны, средства анализа содержимого, средства предотвращения вторжений, антивирусные средства, средства мониторинга и контроля защищенности.

Программное обеспечение портала госуслуг ежегодно проходит сертификацию по требованиям информационной безопасности и отсутствию недекларированных возможностей и переаттестацию по требованиям ФСТЭК на обработку конфиденциальной информации и персональных данных по требованиям.

Персональные данные пользователей портала госуслуг хранятся в Единой системе идентификации и аутентификации (ЕСИА). Это федеральная государственная информационная система, созданная для обеспечения санкционированного доступа участников информационного взаимодействия к информации, содержащейся в государственных информационных системах, муниципальных информационных системах и иных информационных системах. Данная система так же, как и портал госуслуг, аттестована по требованиям ФСТЭК на обработку конфиденциальной информации и персональных данных и реализована с помощью решений, прошедших сертификацию в ФСБ, что гарантирует полное соответствие требованиям законодательства РФ о защите персональных данных, в частности требованиям Федерального закона №152 о защите персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

При этом необходимо помнить, что безопасность определяется не только уровнем защиты портала, но и уровнем защиты рабочего места, с которого осуществляется доступ. В частности, для безопасной работы с порталом госуслуг пользователь должен следовать следующим рекомендациям:

- Использовать на рабочем месте исключительно лицензионное программное обеспечение;
- Устанавливать все необходимые обновления безопасности, рекомендуемые производителем программного обеспечения;
- Устанавливать и регулярно обновлять лицензионное антивирусное программное обеспечение, регулярно проводить проверку на отсутствие вирусов;
- Не загружать программ и данных из непроверенных источников, не посещать сайты сомнительного содержания;
- Не заходить в личный кабинет портала госуслуг со случайных компьютеров, интернет-кафе либо иных недоверенных рабочих мест;
- Не передавать кому-либо токены для авторизации на портале, либо информацию для входа в личный кабинет, следить за сохранностью средств доступа.

Доверять официальным источникам

Злоумышленники могут наживаться на популярных темах: например, манипулировать темой господдержки в связи с коронавирусом или предлагать помощь с оформлением других выплат, когда закон только вышел и еще никем не подписан. СМИ создают ажиотаж, а мошенники этим пользуются.

Доверяйте только официальной информации. Все изменения в законодательстве, размеры выплат и порядок их получения можно узнавать по контактам официальных ведомств и на их сайтах.

Официальные источники Российской Федерации:

- Сервер государственных органов власти http://gov.ru/
- Портал Госуслуг
- Сайт Центрального банка
- Сайт Федеральной налоговой службы
- Страница с официальными контактами ведомств

Проверять случайные сайты, письма и звонки

Официально Госуслуги могут написать на электронную почту, прислать уведомление в приложении или ответить в комментариях соцсетей от имени сообщества. Это нормально, и многие привыкли: так можно вовремя узнать статус заявления или быстрее решить вопрос по сервису без официальных писем. К сожалению, этим пользуются мошенники.

Сайты-двойники. Преступник создает сайт, который внешне напоминает портал Госуслуг. Он в таких же цветах, с такими же кнопками и даже похожим адресом. Но отличия все же есть.

Например, официальный домен госуслуг выглядит так: gosuslugi.ru. Во многих браузерах у него есть замочек в адресной строке: это может значить, что адрес проверенный. Но не всегда: поэтому, если вы видите в интернете похожий сайт, обязательно зайдите на официальный портал вручную.

Официальный адрес портала Госуслуг: https://www.gosuslugi.ru/

Фишинговые ссылки. Вам на почту может прийти письмо с примерно таким содержанием: «Помогите собрать деньги на лечение ребенка» или «Новая акция от Госуслуг: выплаты всем гражданам в связи с коронавирусом». А дальше ссылка, по которой просят перейти и оставить данные, куда придут деньги.

Чаще всего такие письма приходят от мошенников: если перейти по ссылке, на компьютер может попасть вирус. Так злоумышленники получат доступ к персональным данным, а затем оформят на них симкарту, кошелек или возьмут кредит. Не открывайте такие письма и не переходите по ссылкам.

Обращайте внимание на адрес отправителя. Обычно почтовые сервисы помечают проверенные адреса замочками, но это тоже не гарантия. Поэтому смотрите на домен: официальные письма приходят от no-reply@gosuslugi.ru Сообщения могут приходить и в мессенджерах: например, в Вацап или Вайбер. Особенно не доверяйте таким сообщениям и проверяйте ссылки на официальные ресурсы.

Официальные страницы портала Госуслуг в соцсетях:

- Вконтакте
- Одноклассники
- Телеграм-канал

Подозрительные звонки. Стать жертвой можно не только в интернете. Вам могут позвонить и представиться сотрудником Госуслуг, после чего попытаться узнать персональные данные.

Запомните: никогда не сообщайте по телефону личных данных, паролей и номеров банковских карт. Настоящие сотрудники не попросят вас делать тестовые переводы денег, диктовать им код из СМС. Если есть сомнения, что с вами говорит сотрудник Госуслуг, после разговора перезвоните по официальному номеру и уточните информацию.

- Официальный номер службы поддержки Госуслуг: 8 800 100-70-10
- Официальный номер, с которого приходят СМС: 0919

Не обсуждать деньги с незнакомыми

Частый способ обмана: мошенники представляются сотрудниками налоговой и просят оплатить небольшую задолженность. Угрожают штрафами. Из-за незначительной суммы люди соглашаются, так как не хотят тратить время на разбирательства с органами.

Не называйте в переписке никаких реквизитов, не давайте номеров карт и паролей. В официальной переписке с порталом у вас могут попросить только номер заявки, чтобы проверить ее статус, не больше.

Сотрудники Госуслуг никогда не попросят у вас никаких реквизитов для оплаты в соцсетях. Любые задолженности, счета и штрафы можно легко

проверить онлайн. Достаточно зайти на Госуслуги с логином и паролем — на главной странице будет информер со всеми начислениями.

Оплатить штрафы и задолженности можно тут же на портале или в приложении с помощью электронного кошелька, со счета телефона или банковской картой. Проверить штрафы и задолженности

3. РЕКОМЕНДАЦИИ КИБЕРБЕЗОПАСНОСТИ СБЕРБАНКА

https://www.sberbank.ru/ru/person/cybersecurity

Защищаем банк и клиентов

Сбербанк создал уникальную экосистему кибербезопасности на уровне мировых лидеров. Мы пресекаем деятельность мошеннических группировок на самых ранних этапах — в этом нам помогают накопленные данные, высокий профессионализм специалистов, совершенные технологии и сотрудничество с правоохранительными органами.

Ваша кибербезопасность

Защитите себя и свои деньги от злоумышленников

- Куда пожаловаться на мошенников
- Как заблокировать спам и проверить подозрительный телефон
- Приёмы самозащиты от жуликов

Сообщить о мошенничестве
Проверить мошенника

Сервисы кибербезопасности в приложении СберБанк Онлайн

В разделе «Безопасность» мы собрали всё, что поможет вам защитить себя от мошенников: сервисы проверки данных, настройки безопасности, обучающие статьи, видео и тесты.

1. Проверка операций близкого

Сервис «Проверка операций близкого» помогает защитить близких от мошенников. Например, если близкий человек захочет перевести кому-то деньги, банк пришлёт вам уведомление. Вы сможете подтвердить или отклонить перевод, если он показался вам подозрительным.

Как подключить

Зайдите в приложение СберБанк Онлайн → «Профиль» (портрет в левом верхнем углу экрана» → «Настройки» → «Безопасность» → «Проверка операций близкого» и следуйте подсказкам.

Подробнее

2. Проверить входящие звонки

Сервис предупредит о звонках мошенников.

Как подключить

Чтобы разрешить приложению определять вызовы:

На iOS: зайдите в «Настройки» телефона → «Телефон» → «Блокировка и идентификация вызова» → выберите «СберБанк» (или «Настройки» → «Конфиденциальность» → «Отслеживание» → включите «Трекинг-запросы приложениями»).

На Android путь может отличаться в зависимости от модели телефона. Для быстрого подключения отсканируйте QR-код на **странице**.

3. Проверить телефон и почту

Узнайте, не попали ли ваши контакты к мошенникам из-за утечек в разных сервисах. Для проверки используются основной телефон и емейл из профиля СберБанк Онлайн. Если не видите телефона или адреса, добавьте их в своём профиле.

Как проверить

На главном экране приложения СберБанк Онлайн найдите «Безопасность» → «Проверка номера и почты».

4. Закрыть доступ к картам и счетам

Карты. Если вы назвали мошеннику данные своей карты или код из СМС, сразу заблокируйте карту, чтобы никто не смог потратить с неё деньги.

Счета. Если мошенники получили ваши пароли или ПИН-код, скройте вклады и счета, и они станут недоступны в СберБанк Онлайн и банкоматах.

Как закрыть доступ

Главный экран СберБанк Онлайн → «Безопасность» → «Закрыть доступ».

5. Сообщите о мошеннике

Если вас попытались обмануть или вы пострадали от действий мошенников, сообщите об этом нам через специальную форму. Команда кибербезопасности Сбера срочно примет меры.

Как сообщить

Главный экран СберБанк Онлайн → «Безопасность» → «Сообщить о мошеннике».

6. Заблокируйте карту при подозрении на мошенничество

Зайдите в приложение → нажмите на нужную карту на главном экране → «Настройки» → «Заблокировать».

7. Раздел «Не дайте себя обмануть»

Здесь собраны статьи, комиксы и видео, которые просто и понятно объясняют, как мошенники манипулируют своими жертвами.

Пройдите несложные обучающие тесты, чтобы научиться распознавать уловки злоумышленников.

Как найти

Главный экран СберБанк Онлайн → «Безопасность» → «Не дайте себя обмануть».

8. Канал «Осторожно, мошенники!»

Регулярно публикуем самые свежие мошеннические схемы и способы защиты от них.

Как найти

В СберБанк Онлайн в разделе «Диалоги» → закладка «Каналы» или отсканируйте QR-код справа.

Будьте бдительны и осторожны

Мы постоянно блокируем мошеннические сайты с вредоносными программами и доменные имена, с которых мошенники устраивают фишинговые атаки. Но самая надёжная защита — это ваша осведомленность и бдительность.

Осторожно: мошенники используют тему коронавируса как приманку.

- ✓ Если видите в почте письмо со словом «коронавирус» в теме, будьте осторожны и не переходите по ссылкам — там может оказаться сайт-ловушка.
- ✓ Внимательно проверяйте ссылки в письме, особенно короткие. Не оставляйте свои данные на подозрительных сайтах.
- ✓ Доверяйте только официальным аккаунтам Сбербанка в соцсетях и не сообщайте никому пароли из СМС и номера карты — мошенники часто пишут от имени Сбербанка.

Правила личной кибербезопасности

Это должен знать каждый, кто не хочет быть обманутым и лишиться денег:

- ✓ Не сообщайте никому свои пароли, ПИН- и CVV-коды и коды из СМС. Даже сотрудникам банка.
- ✓ Не переходите по подозрительным ссылкам: мошенники могут заразить ваш компьютер или телефон вирусом и украсть ваши данные.
- ✓ Используйте только официальные приложения банка в App Store, Google Play и Microsoft Store.
- ✓ Используйте антивирусы. Приложение Сбербанк Онлайн на Android имеет бесплатный антивирус.
- ✓ Сообщите банку о смене номера мобильного: есть риск, что ваши данные попадут новому владельцу.

- ✓ Проверяйте реквизиты переводов и платежей, которые приходят в СМС от банка.
- ✓ Сбербанк отправляет СМС только с номеров 900 и 9000.
- ✓ С номера 9000 банк проводит СМС-опрос о качестве обслуживания и проводит актуализацию данных.
- ✓ Сообщение может содержать ссылку на портал Центра недвижимости Сбербанка Domclick.ru или опрос Сбербанка.
- ✓ При использовании банкоматов прикрывайте клавиатуру рукой, когда вводите ПИН-код.
- ✓ Не принимайте помощь от незнакомцев, находясь у банкомата, и не совершайте операции под диктовку.
- ✓ Осмотрите банкомат перед использованием и убедитесь, что на нём нет подозрительных устройств.

Вы и кибермошенник: кто кого?

Проверьте себя на знание правил цифровой безопасности.

Пройти тест https://www.sberbank.ru/ru/person/cybersecurity_test .

Узнайте о распространённых приёмах злоумышленников и не дайте им себя обмануть

Ситуация 1. «Звонок из службы безопасности банка»

Вам звонит незнакомец. Номер входящего звонка очень похож на номер банка, а звонящий представляется «сотрудником службы безопасности банка».

Злоумышленники могут поменять одну цифру в номере, которую вы не заметите и подумаете, что это банковский номер. У вас просят конфиденциальные данные

Мошенник сообщает, что «банк выявил подозрительную операцию» или «в системе произошел сбой». Он просит у вас полные данные карты, CVV- или CCV-код, код из СМС или пароли от Сбербанк Онлайн. Это нужно якобы «для сохранности ваших денег».

Как мошенник может вас убеждать

- «Мы звоним с официального номера, проверьте на сайте».
- «В целях конфиденциальности я включаю программу-робот, которая защитит ваши конфиденциальные данные» (вы слышите в трубке лёгкий шелест).
- Для убедительности он называет ваши персональные данные и просит перевести деньги «на защищённый счет, который закреплён за персональным менеджером — это нужно для безопасности, а потом вы сможете вернуть деньги».

Давайте бороться с мошенниками вместе

Вам или вашим близким звонили мошенники и пытались выманить ваши персональные данные? Пришло письмо или сообщение якобы от Сбербанка? Обнаружили поддельный сайт или аккаунт в соцсетях с логотипом банка?

Сообщите нам прямо сейчас: служба безопасности банка примет меры

Вас обманули мошенники? Вы сообщили коды из СМС, данные своей карты, логины или пароли от Сбербанк Онлайн?

Срочно позвоните в банк для консультации с экспертом:

В мобильном приложении: нажмите иконку телефона в левом верхнем углу. Или срочно звоните по номеру 900.

4. РЕКОМЕНДАЦИИ КИБЕРБЕЗОПАСНОСТИ «ЛАБОРАТОРИИ КАСПЕРСКОГО»

Сайт: https://www.kaspersky.ru/resource-center

Определения. Что такое кибербезопасность?

https://www.kaspersky.ru/resource-center/definitions

Кибербезопасность (ее иногда называют компьютерной безопасностью) – это совокупность методов и практик защиты от атак злоумышленников для компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных. Кибербезопасность находит применение в самых разных областях, от бизнес-сферы до мобильных технологий. В этом направлении можно выделить несколько основных категорий.

- **Безопасность сетей**– действия по защите компьютерных сетей от различных угроз, например целевых атак или вредоносных программ.
- **Безопасность приложений**– защита устройств от угроз, которые преступники могут спрятать в программах. Зараженное приложение может открыть злоумышленнику доступ к данным, которые оно должно защищать. Безопасность приложения обеспечивается еще на стадии разработки, задолго до его появления в открытых источниках.
- **Безопасность информации**– обеспечение целостности и приватности данных как во время хранения, так и при передаче.
- **Операционная безопасность**– обращение с информационными активами и их защита. К этой категории относится, например, управление разрешениями для доступа к сети или правилами, которые определяют, где и каким образом данные могут храниться и передаваться.
- **Аварийное восстановление и непрерывность бизнеса** – реагирование на инцидент безопасности (действия злоумышленников) и любое другое событие, которое может нарушить работу систем или привести к потере данных. Аварийное восстановление – набор правил, описывающих то, как организация будет бороться с последствиями атаки и восстанавливать рабочие процессы. Непрерывность бизнеса – план действий на случай, если

организация теряет доступ к определенным ресурсам из-за атаки злоумышленников.

- **Повышение осведомленности**– обучение пользователей. Это направление помогает снизить влияние самого непредсказуемого фактора в области кибербезопасности – человеческого. Даже самая защищенная система может подвергнуться атаке из-за чьей-то ошибки или незнания. Поэтому каждая организация должна проводить тренинги для сотрудников и рассказывать им о главных правилах: например, что не нужно открывать подозрительные вложения в электронной почте или подключать сомнительные USB-устройства.

Масштаб распространения киберугроз.

Год за годом в мире становится все больше угроз и происходит все больше утечек данных. Статистика шокирует: согласно отчету RiskBased Security, только за первые девять месяцев 2019 года было зафиксировано 7,9 миллиардов случаев утечки данных. Эти цифры превышают показатели за тот же период 2018 года более чем в два раза (на 112 %).

Чаще всего утечке данных подвергаются медицинские и государственные учреждения или организации из сферы розничной торговли. В большинстве случаев причина – действия преступников. Некоторые организации привлекают злоумышленников по понятной причине – у них можно украсть финансовые и медицинские данные. Однако мишенью может стать любая компания, ведь преступники могут охотиться за данными клиентов, шпионить или готовить атаку на одного из клиентов.

Компания International Data Corporation прогнозирует, что если количество киберугроз будет расти и дальше, то объем расходов на решения в области кибербезопасности к 2022 году достигнет 133,7 миллиардов долларов США. Правительства разных стран борются с преступниками, помогая организациям внедрять эффективные методы кибербезопасности.

Так, Национальный институт стандартов и технологий США (National Institute of Standards and Technology, NIST) разработал принципы безопасной IT-инфраструктуры. NIST рекомендуют проводить постоянный мониторинг всех электронных ресурсов в реальном времени, чтобы выявить вредоносный код, пока он не нанес вреда, и предотвратить его распространение.

Национальный центр кибербезопасности (National Cyber Security Centre) правительства Великобритании выпустил руководство 10 steps to cyber security (10 шагов к кибербезопасности). В нем говорится о том, насколько важно вести наблюдение за работой систем. В Австралии рекомендации по борьбе с новейшими киберугрозами регулярно публикует Австралийский центр кибербезопасности (Australian Cyber Security Centre, ACSC).

Виды киберугроз

Кибербезопасность борется с тремя видами угроз.

1. **Киберпреступление**– действия, организованные одним или несколькими злоумышленниками с целью атаковать систему, чтобы нарушить ее работу или извлечь финансовую выгоду.
2. **Кибератака** – действия, нацеленные на сбор информации, в основном политического характера.
3. **Кибертерроризм** – действия, направленные на дестабилизацию электронных систем с целью вызвать страх или панику.

Как злоумышленникам удается получить контроль над компьютерными системами?

Они используют различные инструменты и приемы – ниже мы приводим самые распространенные.

Вредоносное ПО

Название говорит само за себя. Программное обеспечение, которое наносит вред, – самый распространенный инструмент киберпреступников. Они создают его сами, чтобы с его помощью повредить компьютер пользователя и данные на нем или вывести его из строя. Вредоносное ПО часто распространяется под видом безобидных файлов или почтовых вложений. Киберпреступники используют его, чтобы заработать или провести атаку по политическим мотивам.

Вредоносное ПО может быть самым разным, вот некоторые распространенные виды:

- **Вирусы –** программы, которые заражают файлы вредоносным кодом. Чтобы распространяться внутри системы компьютера, они копируют сами себя.
- **Троянцы –** вредоносы, которые прячутся под маской легального ПО. Киберпреступники обманом вынуждают пользователей загрузить троянца на свой компьютер, а потом собирают данные или повреждают их.
- **Шпионское ПО –** программы, которые втайне следят за действиями пользователя и собирают информацию (к примеру, данные кредитных карт). Затем киберпреступники могут использовать ее в своих целях.
- **Программы-вымогатели** шифруют файлы и данные. Затем преступники требуют выкуп за восстановление, утверждая, что иначе пользователь потеряет данные.
- **Рекламное ПО –** программы рекламного характера, с помощью которых может распространяться вредоносное ПО.
- **Ботнеты –** сети компьютеров, зараженных вредоносным ПО, которые киберпреступники используют в своих целях.

SQL-инъекция

Этот вид кибератак используется для кражи информации из баз данных. Киберпреступники используют уязвимости в приложениях, управляемых данными, чтобы распространить вредоносный код на языке управления базами данных (SQL).

Фишинг

Фишинг – атаки, цель которых – обманом заполучить конфиденциальную информацию пользователя (например, данные банковских карт или пароли). Часто в ходе таких атак преступники отправляют жертвам электронные письма, представляясь официальной организацией.

Атаки Man-in-the-Middle («человек посередине»)

Это атака, в ходе которой киберпреступник перехватывает данные во время их передачи – он как бы становится промежуточным звеном в цепи, и жертвы об этом даже не подозревают. Вы можете подвергнуться такой атаке, если, например, подключитесь к незащищенной сети Wi-Fi.

DoS-атаки (атаки типа «отказ в обслуживании»)

Киберпреступники создают избыточную нагрузку на сети и серверы объекта атаки, из-за чего система прекращает нормально работать и ею становится невозможно пользоваться. Так злоумышленники, например, могут повредить важные компоненты инфраструктуры и саботировать деятельность организации.

Новейшие киберугрозы

С какими из новейших киберугроз сталкиваются пользователи и организации? Рассмотрим некоторые из тех, что попали в отчеты правительств Великобритании, США и Австралии.

Троянец Dridex

В декабре 2019 года Министерство юстиции США обвинило лидера группы киберпреступников в участии в атаке с использованием зловреда Dridex. Эта кампания затронула общественные, правительственные и деловые структуры по всему миру.

Dridex – банковский троянец с широким набором возможностей, который появился в 2014 году. Он проникает на компьютеры жертв с помощью фишинговых писем и вредоносных программ. Dridex может красть пароли, данные банковских карт и личную информацию пользователей, которые затем используют мошенники. Размер причиненного им финансового ущерба исчисляется сотнями миллионов.

Чтобы защититься, Национальный центр кибербезопасности Великобритании рекомендует устанавливать на устройства последние обновления безопасности и антивирусное ПО свежих версий, а также регулярно выполнять резервное копирование файлов.

Emotet

В конце 2019 года Австралийский центр кибербезопасности предупредил организации о распространении киберугрозы под названием Emotet.

Emotet – сложно устроенный троянец, способный похищать данные, а также загружать вредоносное ПО на устройства. Его жертвами часто становились те, кто использовал простые пароли – это в очередной раз

напомнило пользователям, что нужно использовать более сложные комбинации.

Все, что нужно знать об интернет-угрозах и методах защиты. Узнайте как защитить себя и своих близких в сети.

https://www.kaspersky.ru/resource-center

Защита конечных пользователей

Поговорим о еще одном важном аспекте кибербезопасности – защите конечных пользователей и их устройств (тех, кто использует программу или систему). Часто именно конечный пользователь случайно загружает вредоносную программу на компьютер, ноутбук или смартфон.

Как инструменты кибербезопасности (защитные программы) помогают защитить конечных пользователей и их устройства? В защитных средствах используются криптографические протоколы, которые позволяют шифровать электронную почту, файлы и другие важные данные. Этот механизм не дает киберпреступникам украсть и перехватить данные или получить к ним доступ.

Решения, защищающие конечных пользователей, проверяют их устройства на наличие вредоносного кода, помещают вредоносов на карантин и затем удаляют их из системы. Такие программы могут найти и удалить вредоносный код, спрятанный в основной загрузочной записи (MBR), а также умеют шифровать или полностью стирать информацию на жестком диске.

Защитные средства обнаруживают вредоносные программы в режиме реального времени, многие из них применяют эвристический и поведенческий анализ – следят за действиями вредоноса и его кода. Это помогает бороться с полиморфным и метаморфным вредоносным ПО – вирусами и троянцами, которые могут менять свою структуру. Защитные инструменты умеют изолировать потенциально вредоносное ПО в специальной виртуальной среде (подальше от сети пользователя), чтобы затем проанализировать его поведение и научиться лучше распознавать новые источники угроз.

Профессионалы в области кибербезопасности ищут и анализируют новые угрозы, а затем разрабатывают способы борьбы с ними. Важно научить сотрудников правильно пользоваться защитным ПО. Чтобы защитные средства эффективно выполняли свои функции, они всегда должны быть во включенном состоянии и постоянно обновляться.

Как защититься от атак: полезные советы по кибербезопасности

Предлагаем вам советы о том, как оградить компанию и ее сотрудников от киберугроз.

1. **Обновите программное обеспечение и операционную систему.** Используя новое ПО, вы получаете свежие исправления безопасности.

2. **Используйте антивирусные программы.** Защитные решения, такие как Kaspersky Total Security, помогут выявить и устранить угрозы. Для максимальной безопасности регулярно обновляйте программное обеспечение.

3. **Используйте надежные пароли.** Не применяйте комбинации, которые легко подобрать или угадать.

4. **Не открывайте почтовые вложения от неизвестных отправителей –** они могут быть заражены вредоносным ПО.

5. **Не переходите по ссылкам, полученным по почте от неизвестных отправителей или неизвестных веб-сайтов –** это один из стандартных путей распространения вредоносного ПО.

6. **Избегайте незащищенных сетей Wi-Fi в общественных местах –** в них вы уязвимы для атак Man-in-the-Middle.

Как очистить кеш и удалить файлы cookie в различных браузерах

Когда вы пользуетесь интернетом, браузеры собирают данные о ваших предпочтениях, поисковых запросах и истории просмотров. Чтобы оптимизировать работу вашего браузера, рекомендуется периодически очищать кэш и удалять файлы cookie. В этой статье описано, как очистить историю в разных браузерах.

Что такое кеш?

Кеш – это часть места на жестком диске, предназначенная для хранения файлов браузера, которые, согласно оценкам браузера, могут быть использованы повторно. Без этой функции браузер работал бы медленнее, поскольку при открытии каждого веб-сайта должно было бы загружаться большое количество файлов с нуля, включая такие компоненты, как логотип сайта, фоновые изображения, шрифты, а также технические элементы, такие как CSS, HTML и JavaScript. В совокупности их количество может достигать десятков, сотен или даже тысяч файлов для одного веб-сайта. В кеше эти файлы хранятся локально, поэтому при будущих посещениях веб-сайты будут загружаться быстрее, что улучшит общее впечатление от работы в интернете.

Зачем очищать кеш?

Очистка кеша означает удаление всей сохраненной информации, которая хранилась в кеше, с локального жесткого диска. Ниже перечислен ряд причин, по которым может потребоваться очистить историю просмотров.

Повышение производительности

В зависимости от настроек браузера, кеш может оказаться довольно большим и занимать значительное место на диске компьютера. Чем больше информации хранится в кеше, тем медленнее работает компьютер при просмотре сайтов. Очистка кеша может увеличить время загрузки веб-сайтов, однако повысит производительность устройства.

Просмотр актуальной информации

Теоретически, при каждом повторном посещении сайта, выполняется проверка кеша на предмет того, изменился ли сайт, чтобы отобразить актуальную информацию. Однако это происходит не всегда: иногда происходит загрузка старых сохраненных страниц из кеша, и, следовательно, актуальная информация может не отображаться. Периодическая очистка кеша заставляет браузер запускаться заново, что обеспечивает просмотр актуальных страниц и информации.

Обеспечение безопасности

Очистка кеша может помочь защитить конфиденциальность при использовании общего компьютера. Если не очистить кеш, любой, кто использует компьютер после вас, сможет увидеть вашу историю просмотров в браузере. В кэше также могут храниться личные данные, требуемые для некоторых сайтов. Они могут дать следующему пользователю компьютера доступ к конфиденциальной или личной информации. Временные файлы кеша также могут являться целью рекламных и вредоносных программ, а также вирусов.

Исправление ошибок браузера

Иногда кеш может вызывать проблемы в работе браузера. Например, некоторые сайты могут загружаться медленно или частично, не открываться, возвращать сообщения об ошибках или не реагировать должным образом. Часто такие ошибки можно исправить, очистив кеш, а затем закрыть и повторно открыть браузер.

Зачем удалять файлы cookie?

Файлы cookie – это простые текстовые файлы, которые веб-сайт может хранить в браузере. Они предназначены для идентификации пользователей, хранения данных для входа на сайт и создания персонализированных веб-страниц, учитывающих индивидуальные предпочтения. Более подробная информация о файлах cookie приведена здесь.

Иногда пользователи просматривают настройки файлов cookie или удаляют их в браузере по следующим причинам:

- Повышение безопасности. Злоумышленники могут перехватить файлы cookie, что предоставит им доступ к сеансам браузера и позволит украсть личные данные.
- Защита личной информации. Файлы cookie содержат личные данные. Веб-сайты используют эту информацию для отслеживания интернет-активности, составления детализированного профиля онлайн-привычек и настройки таргетированной рекламы.
- Меры предосторожности при использовании общих компьютеров. Если не удалить файлы cookie после сеанса использования общего компьютера, пользователь, который войдет в систему после вас, сможет

увидеть вашу историю просмотров и даже войти в вашу учетную запись онлайн-банка или интернет магазина, если вы забудете из нее выйти.

- Повышение производительности. При первом посещении веб-сайта, открываемые страницы сохраняются на жестком диске компьютера. Это ускоряет его загрузку при последующих посещениях. Однако со временем может накопиться огромное количество файлов cookie, что замедляет работу системы. Их удаление может помочь повысить производительность.

В чем разница между кешем и файлами cookie?

И кеш, и файлы cookie предназначены для повышения производительности веб-сайтов и удобства работы пользователей за счет хранения данных на устройствах. Однако между ними есть следующие различия:

- Файлы cookie используются для хранения информации о различных аспектах работы пользователя, а кеш используется для ускорения загрузки веб-страниц.
- В файлах cookie хранится такая информация, как пользовательские настройки, а в кеше хранятся файлы ресурсов: аудио, видео или флэш-файлы.
- Срок хранения файлов cookie обычно ограничен, а кеш хранится на устройстве пользователя до тех пор, пока не будет удален вручную.

Как очистить кеш и удалить файлы cookie

Как очистить кеш браузера? В Internet Explorer, Edge, Google Chrome и Mozilla Firefox кеш можно быстро очистить с помощью сочетания клавиш: по нажатию **Ctrl+Shift+Delete** откроется соответствующее окно. Не забудьте закрыть браузер и повторно открыть его после очистки кеша и удаления файлов cookie.

Далее приведены способы очистки истории поиска в различных браузерах.

Удаление истории в Google Chrome

1. Откройте меню **Инструменты** (щелкните три вертикальные точки в правом верхнем углу).
2. Выберите пункт **История.**
3. Слева выберите вариант **Очистить историю**. Установите для параметра **Временной диапазон** значение **Все время**. Установите флажки **Файлы cookie и другие данные сайтов** и **Изображения и другие файлы, сохраненные в кеше** и нажмите на кнопку **Удалить данные.**
4. На компьютере с операционной системой Windows закройте и повторно откройте Chrome, чтобы сохранить изменения. На компьютере Apple, перейдите в меню **Chrome** в верхней строке меню и выберите пункт **Выход**, чтобы изменения вступили в силу.

Удаление истории в Google Chrome для iOS

1. Откройте Google Chrome на iOS-устройстве.
2. Нажмите на панель меню в правом нижнем углу.
3. Выберите **Настройки**.
4. Выберите пункт **Конфиденциальность.**
5. Выберите **Файлы cookie**, **Данные сайтов** и **Изображения и файлы, сохраненные в кеше**. Установите для параметра **Временной диапазон** значение **Все время.**
6. В нижней части экрана нажмите на кнопку **Очистить историю**.

Подтвердите ваше действие, повторно нажав на кнопку **Очистить историю**.

Удаление истории в Firefox

1. Перейдите на панель **Инструменты**.
2. Выберите пункт **Настройки**.
3. В меню слева выберите пункт **Приватность и Защита**.
4. В разделе **Куки и данные сайтов**, нажмите на кнопку **Удалить данные**.
5. Выберите два варианта и нажмите на кнопку **Удалить**.

На компьютере с операционной системой Windows закройте и повторно откройте Firefox, чтобы сохранить изменения. На компьютере Apple, перейдите в меню **Firefox** в верхней строке меню и выберите пункт **Выход**, чтобы изменения вступили в силу.

Удаление истории в Safari для macOS

1. Выберите **Safari** в верхней строке меню.
2. Выберите пункт **Настройки.**
3. Перейдите на закладку **Конфиденциальность**.
4. Выберите **Управление данными веб-сайта.**
5. Нажмите на кнопку **Удалить все**.
6. Нажмите на кнопку **Удалить сейчас.**
7. Выберите **Safari** в верхней строке меню.

Выберите пункт **Выход**, чтобы закрыть Safari и сохранить изменения.

Удаление истории в Safari для iOS – удаление файлов cookie на iPhone

1. Перейдите в приложение Настройки на устройстве.
2. Прокрутите вниз и откройте меню **Safari**.
3. Прокрутите вниз и выберите **Очистить историю и данные сайтов.**
4. Отобразится всплывающее окно с вопросом, хотите ли вы очистить историю и данные. Выберите **Очистить историю и данные**.

После очистки кеша и удаления файлов cookie кнопка Очистить историю и данные сайтов станет серой.

Удаление истории в Microsoft Edge для Windows 10

1. Перейдите в меню **Инструменты** (три пунктирные линии в правом верхнем углу) и откройте меню **Параметры**.
2. Выберите пункт **Конфиденциальность, поиск и службы** в меню слева.
3. В разделе **Очистка данных браузера** нажмите **Выбор элементов для удаления**.
4. Выберите **Файлы cookie и другие данные сайтов** и **Изображения и файлы, сохраненные в кеше**.
5. Нажмите на кнопку **Очистить сейчас.**
6. Закройте Microsoft Edge, чтобы изменения вступили в силу.

VPN помогает обеспечить конфиденциальность в интернете без дополнительных действий

Некоторым пользователям не нравится удалять файлы cookie, поскольку для них важно отсутствие необходимости ввода учетных данных при каждом входе на часто используемые сайты. Для пользователей, стремящихся сохранить конфиденциальность при работе в интернете, отличным вариантом может стать виртуальная частная сеть (VPN). VPN, например, Kaspersky Security Connection, шифрует данные, передаваемые на компьютер и с него, блокирует перехват файлов cookie трекерами рекламы и удаляет личную информацию.

Статьи по теме:

- Что такое VPN и как она работает
- Что такое «похищение браузера»?
- Как сохранить конфиденциальность в сети при совпадении деловых и личных целей
- Как хакеры нарушают конфиденциальность в сети
- Как избежать рисков для безопасности в публичных сетях Wi-Fi

Угрозы во время пандемии коронавируса

1. COVID-19: Как защититься от киберугроз, связанных с коронавирусом.

Пандемия COVID-19 вызвала новую волну атак фишеров, мошенников и других злоумышленников в интернете. «Лаборатория Касперского» расскажет, как от них защититься.

https://www.kaspersky.ru/resource-center/threats/coronavirus-how-to-stay-safe-hackers-scammers

2. Удаленная работа: 10 советов по онлайн-безопасности во время пандемии COVID-19

Работаете из дома? Самое время позаботиться об онлайн-безопасности и защититься от утечки данных и от мошенников. Для этого следуйте 10 нашим советам

https://www.kaspersky.ru/resource-center/threats/remote-working-how-to-stay-safe

5. МОШЕННИЧЕСТВО С БАНКОВСКИМИ КАРТАМИ ПРИМЕРЫ ОТ TADVISER

http://www.tadviser.ru

TADVISER приводит хорошие рекомендации и примеры на основе информации Тинькофф-банка

По данным Тинькофф-банка, чтобы обезопасить себя от мошенников, необходимо соблюдать следующие меры безопасности:

✓ Нужно всегда держать в тайне следующие данные: коды из SMS и PUSH-уведомлений, PIN-код карты, контрольные вопросы, данные карты, включая срок действия и трехзначный код. Нельзя также раскрывать персональные данные: отчество, место и год рождения, данные паспорта.

✓ Если кто-то позвонил сам, не следует ему доверять, даже если он представился сотрудником банка. Нужно перезвонить в банк в случае подозрительного звонка или сообщения от банка.

✓ Не нужно скачивать никакие программы на смартфон по просьбе незнакомцев и тем более предоставлять им доступ к ним.

✓ Не нужно носить записанный пин-код рядом с картой. Лучше подключить оповещения об операциях и настроить лимиты на траты.

✓ Для быстрой связи с банком нужно заранее сохранить его номера в телефоне.

✓ Если карта пропала — нужно сразу же связаться с банком, заблокировать карту, проверить операции и обратиться в банк для выпуска карты.

✓ Если украли деньги со счета — нужно связаться с банком и описать ситуацию. После чего — написать заявление в полицию и отправить в банк талон о принятии заявления

✓ Если пропал телефон — нужно связаться с банком для блокировки приложения и удаления данных карты со смартфона. Также нужно немедленно обратиться к сотовому оператору для блокировки сим-карты и проверить последние операции.

✓ Как обезопасить себя от кражи персональных данных

✓ Всегда рвите или иным способом уничтожайте ставшие ненужными документы, содержащие ваши персональные данные, ни в коем случае не выбрасывайте их целиком.

- ✓ Ни в коем случае не реагируйте на "холодные звонки" и электронные сообщения, в которых вас просят предоставить реквизиты счета, PIN-коды, пароли или персональные данные.
- ✓ Не сообщайте о себе слишком много сведений в социальных сетях, например, клички домашних животных, которые вы можете использовать в качестве паролей.
- ✓ Регулярно отслеживайте почту, чтобы знать, когда ожидать важных финансовых или иных документов, которые могут содержать ваши персональные данные и принимайте меры в случае их отсутствия.
- ✓ При переезде не поленитесь дойти до почты и предупредить их о необходимости переадресации вашей почты.
- ✓ Всегда используйте надежные уникальные пароли для максимально возможного количества учетных записей в интернете, а в идеале – индивидуальный пароль для каждой из них. В самом крайнем случае придумайте уникальные пароли для каждого типа поставщиков услуг, таких как финансовые учреждения, интернет-магазины и электронная почта.
- ✓ Не храните логин и пароль на своем смартфоне: в электронном сообщении, в виде заметки или для "автоматического заполнения" при открытии интернет-сайта или приложения. Эта информация станет золотой жилой для мошенников в случае утери или кражи вашего телефона.
- ✓ Не ленитесь проверять выписки по банковским счетам и картам на предмет подозрительных транзакций.
- ✓ Регулярно проверяйте свою Кредитную историю: там указаны все ваши действия по кредитам, так что вы сможете выявить расходы, не имеющие к вам отношения.

Схемы мошенничества

Типичные и нетипичные схемы обмана

По данным Тинькофф существует несколько типичных схем обмана:

- ✓ При добровольном переводе средств клиентом
- ✓ Покупки в интернете. Клиент находит объявление о продаже товара или услуг. Переводит деньги, мошенники перестают выходить на связь.
- ✓ Покупки в интернете с подменой формы. Эта схема распространена при покупках на различных сайтах объявлений. Мошенники не просят перевести деньги за товар, а отправляют клиенту ссылку с формой на оплату - она вызывает больше доверия. Используя уязвимости в протоколе, мошенники подменяют название торговой точки. Клиент предполагает, что совершает покупку, но на самом деле переводит деньги на карту.
- ✓ «Близкий человек попал в беду». В соцсетях пишет родственник или друг. Он попал в непростую ситуацию и ему срочно нужны деньги. Так действуют мошенники, взломав аккаунты.
- ✓ При разглашении банковских данных

✓ Служба безопасности банка. Клиенту поступает звонок или SMS с просьбой перезвонить. Мошенники представляются службой безопасности банка, говорят, что зафиксирована попытка списания денег со счета клиента, выясняют данные карты и коды подтверждения и списывают деньги со счета.

✓ Лотерея или опрос. Клиент видит рекламу в интернете или таргетированную рассылку: можно получить вознаграждение, поучаствовав в лотерее или пройти опрос. Для этого нужно заполнить небольшую форму. Клиент вводит данные карты — мошенники списывают средства, либо получают данные для последующих попыток обмана.

✓ Продажа в интернете. Клиент размещает объявление о продаже товара. Мошенники звонят и узнают данные карты продавца под предлогом необходимости совершить перевод за товар. Далее они списывают деньги с карты, узнав у продавца код подтверждения (якобы он нужен для зачисления). Другой вариант этой схемы — использование подложного сервиса «безопасной сделки» в интернете.

Также в Тинькофф выделили следующие нетипичные схемы обмана:

✓ Черные брокеры. Клиенту поступает предложение заработать на инвестициях. Он связывается с лжеброкерами и переводит им деньги для игры на бирже. Сумма на «брокерском» счете начинает быстро расти. Клиент хочет вывести средства, но для этого нужно заплатить дополнительную комиссию. Он переводит деньги — мошенники пропадают.

✓ Программы удаленного доступа. Звонит «служба безопасности банка»: на устройстве клиента обнаружен вирус, необходимо скачать антивирус и сканировать гаджет. Во время сканирования устройство, якобы, нельзя использовать, так как вирус может распространиться дальше. На самом деле клиент скачивает программу удаленного доступа, а во время «проверки» мошенники получают доступ к мобильному банкингу и выводят средства клиента.

✓ Безопасный счет. Звонок от «службы безопасности»: произошла утечка данных, в ней замешаны сотрудники. Необходимо снять деньги через безопасный банкомат банка-партнера и перевести их на специальный страховочный счет.

✓ Другим вариантом этой схемы является сценарий, когда преступники предлагают сразу перевести деньги на счет, не снимая их в банкомате. За причиненные неудобства клиенту предлагается вознаграждение. Мошенники просят не отключать телефонную связь во время операций. Предупреждают, что "банк" не несет ответственность за сохранность денег по условиям обслуживания счета: если их не снять, они могут пропасть.

✓ Знакомства в сети. На сайте знакомств девушка предлагает сходить в кино. Отправляет ссылку на сайт-однодневку VIP-кинотеатра. Клиент покупает билеты, на этом знакомство завершается.

✓ Автоматическая голосовая служба банка. Звонок из «банка»: был зафиксирован вход в личный кабинет из другого города или страны. В рамках мер по безопасности необходимо назвать номер карты для идентификации. Мошенники предупреждают, что сейчас поступит код по SMS, но его никому нельзя называть. После чего переключают на голосовую службу. Клиент доверяет голосу робота и вводит код в тональном режиме. Мошенники меняют пароль и логин в его личном кабинете и выводят деньги.

Безопасность "интернет вещей"?
https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things)

Что такое "интернет вещей"?
Мир стал цифровым. Сотовые телефоны теперь обычное дело, в школах планшеты заменили тетради, а компании разрабатывают технологии нового поколения, например, автомобили без водителя.
Кажется, все связано между собой, особенно в бизнесе. Будь то автоматические системы безопасности или ноутбуки - количество устройств, подключенных к сети и работающих вместе, только растет. По последним данным, к 2020 году к Интернету будет подключено около 20,4 миллиарда устройств. Для такого рода «взамодействия» есть специальный термин - Интернет вещей (Internet of Things - IoT).
Хотя термин уже в обиходе больше 10 лет, не все до сих пор полностью понимают, что на самом деле он означает и почему он так важен для бизнеса и потребителей.
Термин "интернет вещей" (IoT) - означает взаимодействие устройств, подключенных к Интернету и "общающихся" между собой. Вы, вероятно, сейчас подумали о таких вещах, как ноутбук или умный телевизор, но IoT охватывает значительно более разнообразные устройства, например, электронику, которая никогда ранее не была подключена к сети - домашние холодильники, кофемашины, стиральные машины и так далее. Интернет вещей - это все (даже необычные устройства), которые могут подключаться к Интернету. В наши дни почти любое устройство с выключателем потенциально может подключаться к Интернету, что делает его частью IoT.

Почему все сегодня говорят об «интернете вещей»?
"Интернет вещей" - актуальная тема на сегодняшний день, потому что мы не понимаем, сколько вещей может быть подключено к Интернету и как это

может повлиять на повседневную жизнь. Развитие технологий за последнее десятилетие способствовало таким факторам:

- Способы создания технически «умных» устройств стали более доступными
- Возросло число Wi-Fi - совместимых продуктов
- Количество пользователей смартфонами во всем мире резко увеличилось
- Появились возможности использовать смартфон как устройство, управляющее другими устройствами
- Именно поэтому IoT - больше не профессиональный IT-сленг. Это термин, который должен знать в первую очередь каждый владелец бизнеса.
- Прикладное использование "интернета вещей". Какие приложения наиболее часто используются на рабочем месте?
- Исследования показывают, что IoT- устройства способствуют повышению эффективности работы предприятия. Производительность труда сотрудников, дистанционный мониторинг и отлаженные процессы являются одними из главных преимуществ IoT для компаний.

Но как же выглядит интернет вещей внутри компании? Каждая компания имеет свои особенности, но вот несколько примеров использования IoT на работе:

- Умные замки позволяют руководителю предприятия открывать дверь со своего смартфона, пропуская сотрудника на рабочее место в субботу.
- Интеллектуальные термостаты и фонари включаются и выключаются в нужное время, чтобы сэкономить на расходах на электроэнергию.
- Голосовые помощники, такие как Siri или Alexa, открывают приложения, которые позволяют вам, например, делать заметки, устанавливать напоминания, получать доступ к своему календарю или отправлять электронные письма.
- Подключенные датчики внутри принтеров определяют низкий уровень тонера и автоматически размещают заказ на его пополнение.
- Камеры видеонаблюдения, которые позволяют транслировать контент через Интернет.

Зачем нужно знать о безопасности интернета вещей?

Подключенные устройства могут значительно повысить эффективность вашего бизнеса, но все, что подключено к Интернету, может быть уязвимо для кибератак. Киберпреступники могут найти способ использовать информацию, собранную на разных точках внутри IoT-экосистемы - от корпоративных серверов до облачного хранилища. Это не значит, что вы должны срочно заменить свой рабочий планшет на ручку и бумагу. Это значит, что вы должны

серьезно относиться к безопасности технологии интернета вещей. Вот несколько советов:

- Делайте вкладки на мобильных устройствах.
- Убедитесь, что мобильные устройства, например, планшеты регистрируются и блокируются в конце каждого рабочего дня. Если планшет утерян, данные и информация могут стать доступными злоумышленникам и использованы ими в ненадлежащих целях. Обязательно используйте надежный пароль или биометрический пароль, чтобы никто не мог войти в ваше устройство, если оно утеряно или украдено. Используйте защитный продукт, позволяющий ограничивать приложения, которые будут работать на устройстве, разделять деловые и личные данные и стирать корпоративную информацию в случае кражи устройства.
- Установите автоматические обновления антивируса.

Вам нужно программное обеспечение для всех устройств для защиты от вирусов, которые предоставляют хакерам доступ к вашей системе и данным. Настройте автоматические обновления антивируса для защиты устройств от кибератаки.

- Требуйте использования надежных логинов для входа.

Многие люди используют одинаковые логин и пароль на каждом из своих устройств. Так их легче запомнить. А киберпреступникам легче взломать. Убедитесь, что каждый логин уникален для каждого сотрудника и требуйте использования надежных паролей. Всегда меняйте пароль по умолчанию на новых устройствах. Никогда не используйте один и тот же пароль на разных устройствах.

- Разверните сквозное шифрование.

Подключенные устройства общаются друг с другом, и когда они это делают, данные передаются от одного устройства к другому. Вам нужно зашифровывать данные в каждой точке пересечения. Другими словами, вам необходимо сквозное шифрование для защиты информации во время ее перемещения от точки к точке.

- Убедитесь, что обновления устройства и программного обеспечения доступны, и устанавливайте их вовремя.

При покупке устройства необходимо убедиться, что производитель предоставляет обновления. Устанавливайте обновления, как только они становятся доступны. По возможности используйте автоматические обновления, как указано выше.

- Отслеживайте доступные функции устройства и отключайте функции, которыми не пользуетесь.

Проверьте доступные функции на своих устройствах и отключите те, которые вы не собираетесь использовать, чтобы уменьшить потенциальные возможности атаки.

- Выберите опытного поставщика решений кибербезопасности.

Вы хотите, чтобы технология интернета вещей способствовал развитию вашего бизнеса, а не вредила ему. Обратитесь за помощью к авторитетному поставщику решений кибербезопасности и антивирусной защиты, который имеет опыт борьбы с уязвимостями и предоставляет уникальные решения для предотвращения кибератак.

Интернет вещей больше не технологическое увлечение. Все больше организаций реализовывают свой потенциал, используя подключенные устройства. Но о безопасности забывать нельзя. Когда вы создаете свою IoT-экосистему, убедитесь, что ваша компания, данные и процессы защищены.

6. ДОПОЛНЕНИЯ (2021 – 2022 г.г.)

ЦБ РФ предупредил о новой схеме мошенничества с "компенсациями потерь от мошенников"

https://www.tadviser.ru/index.php

В конце мая 2022 года в Центральном банке РФ рассказали о новой схеме мошенничества в стране. Злоумышленники начали предлагать россиянам «компенсации», если они стали жертвой других мошенников.

Как поясняется в Telegram-канале регулятора, схема работает следующим образом: злоумышленники просят жертву заполнить форму с личными и финансовыми данными, чтобы якобы проверить полагающуюся сумму возврата и оформить его. А затем, получив эти данные, похищают у человека деньги.

Чтобы якобы вернуть пострадавшему похищенные у него деньги, мошенники создают специальные сайты, ссылки на которые направляют по электронной почте, через смс или мессенджеры. Иногда аферисты звонят с предложением оформить компенсацию за похищенные средства.

Вернуть их в такой ситуации невозможно, отмечают в ЦБ. Если же деньги списали без согласия клиента, он не переводил их самостоятельно и не сообщал мошенникам свои личные и финансовые данные, необходимо заблокировать карту и обратиться в банк.

Как сообщил директор департамента информационной безопасности Банка России Вадим Уваров на встрече Ассоциации банков России, это так называемый вариант схемы хищения «обман на обмане». По его словам, с начала мая 2022 года ЦБ инициировал блокировку 38 интернет-ресурсов, предлагающих «различные компенсации, в том числе возврат украденных мошенниками денег». ЦБ в мае 2022 года инициировал блокировку в общей сложности более 25 тыс. мошеннических телефонных номеров, что на 13% больше, чем в апреле, и в три раза больше, чем в марте 2022 года.

Роскачество предупредило о новом виде мошенничества с банковскими картами

Роскачество предупредило о мошеннических сайтах, предлагающих проверку скомпрометированных банковских карт. Об этом стало известно 15 марта 2022 года.

После публикаций в СМИ о том, что злоумышленники слили в теневой интернет данные более чем 100 000 российских банковских карт, в сети начали появляться мошеннические сайты, которые предлагают проверить данные карты пользователя на соответствие слитой базы. Реклама подобных сервисов активно идет в социальных сетях и Telegram-каналах. Рекламная рассылка затрагивает не только владельцев сообществ и групп о финансах, но и пользователей, максимально далеких от банковских терминов. Это значит, что попасть на эту удочку может кто угодно.

Фейковые сайты имеют схожую структуру: держателю карты предлагают ввести данные своих карт, якобы для проверки того, не попалили они в руки злоумышленника. Сервис использует максимально циничный подход. После ввода своих платежных данных пользователь передает свои данные мошенникам, списание средств с карты может произойти сразу.

Также платежные данные могут попасть в руки мошенников, если использовать бесплатный и малопопулярный сервис VPN. Существует риск, что после активации сервиса данные вашей карты будут скомпрометированы.

Мошенники в России для дальнейшего обмана начали переводить деньги потенциальным жертвам

В феврале 2022 года стало известно о том, что мошенники в России для дальнейшего обмана начали переводить деньги потенциальным жертвам. О новой схеме мошенничества «Известиям» рассказал директор по безопасности Почта Банка Станислав Павлунин.

Преступники создают сайты-клоны настоящих инвестиционных компаний для торговли на бирже. Затем они убеждают россиян зарегистрироваться в личном кабинете и перевести средства якобы на брокерский счет. Затем на карту жертвы приходит сумма в 10-15 тыс. рублей. Поверив в легкий заработок, многие впадают в эйфорию и переводят лжеброкеру гораздо большие суммы, в том числе взятые в кредит, после чего мошенники исчезают.

Приемы социальной инженерии

- Типичное мошенничество такого рода выглядит следующим образом: жертве звонит преступник, представляющийся сотрудником банка. По его словам, деньги пользователя в опасности: его личный кабинет только что попытались взломать, со счета выводились средства. Служба безопасности готова спасти ситуацию при небольшом содействии самого клиента банка: к

примеру, ему следует установить программу удаленного управления. После этого мошенник сам получает доступ к приложениям и выводит деньги со счета. Как правило, преступники звонят с «номеров банков», используя особые программы для изменения телефона, а также сообщают жертве некоторую персональную информацию, чтобы втереться в доверие, — такие данные можно легко купить в сети.

- Связываясь с жертвой, злоумышленники вводят ее в заблуждение и выманивают банковские реквизиты и пароли. Нередко они даже напрямую просят сделать денежный перевод. Инструментов у них немало: известны случаи обмана через СМС-сообщения, соцсети, телефонные вызовы. Дополнительной тенденцией становится установка механизма удаленного управления: грабители уговаривают загрузить на телефон определенную программу и запустить ее, и через нее полностью захватывают мобильное устройство.
- Пользователям в интернете обещают крупную сумму за участие в той или иной акции или прохождение опроса. Но, чтобы получить деньги, человек сначала должен оплатить «комиссию» или «сервисный сбор» (обычно сумма небольшая, чтобы не вызвать подозрений. После этого пользователь не только не получает выигрыш, но и прощается с «комиссией», а его платежные данные оказываются в руках злоумышленников. Чаще всего мошенники притворяются крупными компаниями и банками, но бывают и случаи со знаменитостями.

Вот случай применения приемов социальной инженерии на территории ХМАО-Югры.

Жительница Белоярского перевела на счет мошенников, которые представились специалистами Сбербанка, 5,5 млн рублей, сообщило управление МВД по ХМАО. Накануне женщине позвонила якобы сотрудница Сбербанка и уточнила, производила ли на данный момент пользователь карты переводы. «Югорчанка опровергла данную информацию. В ответ на это специалист предостерегла гражданку от действий мошенников и посоветовала оперативно перевести денежные средства на различные резервные банковские ячейки. Гражданка была уверена, что общается с представителем Сбербанка, испугавшись за свои сбережения, последовала рекомендациям девушки и перечислила деньги на счета, которые ей посредством мессенджера WhatsApp указала „доброжелательный“ специалист банка. Таким образом, югорчанка лишилась порядка 5,5 млн рублей», — говорится в сообщении полиции.

https://www.znak.com/2020-11-02/v_hmao_pensionerka_perevela_moshennikam_5_5_mln

Указ Президента РФ от 02.07.2021 г. № 400 "О стратегии национальной безопасности Российской Федерации".

Это базовый документ стратегического планирования, определяющий национальные интересы и стратегические национальные приоритеты России, цели и задачи госполитики в области обеспечения национальной безопасности и устойчивого развития страны на долгосрочную перспективу. Прежняя редакция была утверждена указом 31 декабря 2015 года и утратила силу.

В документе перечислены девять стратегических национальных приоритетов: сбережение народа, оборона, государственная и общественная безопасность, информационная безопасность, экономическая безопасность, научно-технологическое развитие, экологическая безопасность, защита традиционных ценностей, стратегическая стабильность.

Цель обеспечения информационной безопасности - укрепление суверенитета России в информационном пространстве.

Эта цель достигается благодаря формированию безопасной среды оборота достоверной информации. В число задач также входит, в частности, повышение защищенности российского сегмента интернета, снижение до минимально возможного уровня количества утечек персональных данных, обеспечение приоритетного использования в информационной инфраструктуре российских технологий и оборудования.

В документе указывается:

56. Целью обеспечения информационной безопасности является укрепление суверенитета Российской Федерации в информационном пространстве.

57. Достижение цели обеспечения информационной безопасности осуществляется путем реализации государственной политики, направленной на решение следующих задач:

1) формирование безопасной среды оборота достоверной информации, повышение защищенности информационной инфраструктуры Российской Федерации и устойчивости ее функционирования;

2) развитие системы прогнозирования, выявления и предупреждения угроз информационной безопасности Российской Федерации, определения их источников, оперативной ликвидации последствий реализации таких угроз;

3) предотвращение деструктивного информационно- технического воздействия на российские информационные ресурсы, включая объекты критической информационной инфраструктуры Российской Федерации;

4) создание условий для эффективного предупреждения, выявления и пресечения преступлений и иных правонарушений, совершаемых с использованием информационно-коммуникационных технологий;

5) повышение защищенности и устойчивости --функционирования единой сети электросвязи Российской Федерации, российского сегмента сети "Интернет", иных значимых объектов информационно-коммуникационной инфраструктуры, а также недопущение иностранного контроля за их функционированием;

6) снижение до минимально возможного уровня количества утечек информации ограниченного доступа и персональных данных, а также уменьшение количества нарушений установленных российским законодательством требований по защите такой информации и персональных данных;

7) предотвращение и (или) минимизация ущерба национальной безопасности, связанного с осуществлением иностранными государствами технической разведки;

8) обеспечение защиты конституционных прав и свобод человека и гражданина при обработки персональных данных, в том числе с использованием информационных технологий;

9) укрепление информационной безопасности Вооруженных Сил, других войск, воинских формирований и органов, а также разработчиков и изготовителей вооружения, военной и специальной техники;

10) развитие сил и средств информационного противоборства;

11) противодействие использованию информационной инфраструктуры Российской Федерации экстремистскими и террористическими организациями, специальными службами и пропагандистскими структурами иностранных государств для осуществления деструктивного информационного воздействия на граждан и общество;

12) совершенствование средств и методов обеспечения информационной безопасности на основе применения передовых технологий, включая технологии искусственного интеллекта и квантовые вычисления;

13) обеспечение приоритетного использования в информационной инфраструктуре Российской Федерации российских информационных технологий и оборудования, отвечающих требованиям информационной безопасности, в том числе при реализации национальных проектов (программ) и решении задач в области цифровизации экономики и государственного управления;

14) укрепление сотрудничества Российской Федерации с иностранными партнерами в области обеспечения информационной безопасности, в том числе в целях установления международно- правового режима обеспечения безопасности в сфере использования информационно-коммуникационных технологий;

15) доведение до российской и международной общественности достоверной информации о внутренней и внешней политике Российской Федерации;

16) развитие взаимодействия органов публичной власти, институтов гражданского общества и организаций при осуществлении деятельности в области обеспечения информационной безопасности Российской Федерации.

12 июля 2022 года распоряжением Правительства Ханты-Мансийского автономного округа – Югры № 479-рп внесены изменения в распоряжение Правительства Ханты-Мансийского автономного округа

– Югры от 2 июля 2021 года № 359-рп «О Стратегии цифровой трансформации Ханты-Мансийского автономного округа – Югры».

https://admhmao.ru/dokumenty/pravovye-akty-gubernatora/

В Стратегии определено, что информационная безопасность – это состояние защищенности информации (обеспечены конфиденциальность, доступность и целостность) и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

Целью цифровой трансформации Ханты-Мансийского автономного округа – Югры является повышение качества жизни населения, улучшение условий для ведения экономической деятельности организаций и обеспечение эффективности системы государственного и муниципального управления на основе широкомасштабного использования цифровых технологий.

К долгосрочным целям цифровой трансформации отраслей экономики и социальной сферы относятся:

развитие регионального законодательства;
развитие человеческого капитала;
развитие благоприятной бизнес-среды для цифровой трансформации;
развитие и использование информационных систем;
развитие цифровой инфраструктуры;
обеспечение доверия и безопасности в цифровой экономике.

Для успешного достижения целей цифровой трансформации должны быть решены следующие задачи:

1. Создание условий для подготовки специалистов цифровой экономики, развитие системы образования, способной динамично отвечать на новые технологические вызовы.
2. Совершенствование системы финансовой и организационной поддержки инновационной деятельности организаций, функционирующих в сфере создания, развития и использования цифровых технологий в автономном округе.
3. Повышение активности и роли малого и среднего предпринимательства в процессе цифровой трансформации.
4. Развитие безопасной информационной инфраструктуры для обеспечения цифровой трансформации отраслей экономики, социальной сферы и государственного управления.
5. Создание и развитие цифровых платформ.
6. Создание и развитие экосистемы обмена данными для развития технологий искусственного интеллекта.

7. Трансформация государственного управления в том числе при предоставлении государственных и муниципальных услуг с использованием возможностей новых цифровых технологий.
8. Формирование у населения необходимых цифровых навыков для жизни в цифровом мире.

Достижение поставленных целей цифровой трансформации может быть измерено интегральным показателем, например таким как цифровая зрелость.

Как измерять уровень цифровой зрелости на уровне государства пояснил вице-премьер Дмитрий Чернышенко: «Проще говоря, цифровая зрелость отрасли в первую очередь определяется количеством специалистов, использующих в своей работе ИТ-продукты, и объемом отраслевых вложений в использование и внедрение цифровых решений. Отмечу также, что уровень цифровой зрелости — одна из самых наглядных шкал с точки зрения приложения государственных усилий по развитию ИТ-отрасли. Благодаря этому параметру разработанные меры государственной поддержки отвечают конкретным индустриальным запросам и закрывают реальные потребности бизнеса, работая как лекарство: строго дозированно и с учетом всех показателей «анализа крови». Наша задача — вывести экономику, социальную сферу и госуправление России на уровень, где цифровая среда окончательно сформирована, абсолютное большинство процессов автоматизировано, а весь потенциал цифровых технологий, будь то искусственный интеллект, большие данные, облачные вычисления и т. д., полностью реализован на благо страны и каждого человека».

В докладе Департамента информационных технологий и цифрового развития Югры за 2022 год отмечается, что значительное внимание в автономном округе уделяется вопросам информационной безопасности.

В целях качественного обнаружения и локализации компьютерных атак на базе автономного учреждения «Югорский НИИ информационных технологий», в качестве инновационного решения в автономном округе создан Центр кибербезопасности (далее – Центр). В настоящее время Центр системно отслеживает различные события в информационных системах, а также выявляет несанкционированные действия злоумышленников. Персонал Центра проводит анализ инцидентов информационной безопасности, а также выполняет комплекс работ по обнаружению, предупреждению и ликвидации последствий компьютерных атак.

Центр взаимодействует с Национальным координационным центром по компьютерным инцидентам.

Центр позволяет проводить единую техническую политику обеспечения информационной безопасности и централизованно управлять средствами защиты информации: обнаружения вторжений, защиты от несанкционированного доступа, межсетевого экранирования, антивирусной защиты и других.

В 2023 году запланировано продолжить работу по оснащению Центра средствами контроля и к существующим элементам комплексной централизованной системы защиты информации продолжить работу по оснащению Центра средствами контроля и к существующим элементам комплексной централизованной системы защиты информации.

В 2022 году Депинформтехнологий Югры на системной основе проводит работы по тестированию на проникновение в информационные системы (пен-тесты), используя методы и средства, которыми пользуются профессиональные злоумышленники.

В ходе пен-тестов выявляются потенциальные уязвимости систем и разрабатывается комплекс мер по их устранению.

Важно отметить, что государственные информационные системы органов власти автономного округа подключены к «Государственной системе обнаружения и предотвращения компьютерных атак» посредством сервиса обслуживания предприятия-лицензиата ФСТЭК России и ФСБ России.

В целом, в 2022 году система защиты информации функционировала устойчиво, без сбоев. Случаев простоя информационных систем от воздействия компьютерных атак не выявлено.

Актуальные киберугрозы: I квартал 2022 года

https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q1/#id2

Компания Positive Technologies подготовила анализ по итогам I квартала 2022 года:

- Количество атак увеличилось на 14,8% по сравнению с IV кварталом 2021 года. При этом увеличилась доля массовых атак: теперь их количество составляет 33% от общего числа.
- Доля атак на частных лиц остается на прежнем уровне, составляя 15% от общего числа. Методы и мотивы атак не претерпевают существенных изменений.
- Чаще всего в результате атак организации сталкиваются с утечкой конфиденциальной информации (45%) и нарушением основной деятельности (30%). В атаках на частных лиц чаще всего были скомпрометированы конфиденциальные данные (55%), также пользователи могли понести финансовые потери (25%).
- Вырос интерес к веб-ресурсам: доля атак на них увеличилась до 22% от общего количества по сравнению с 13%, наблюдаемыми в IV квартале 2021 года.
- В пятерке наиболее атакуемых отраслей оказались СМИ: доля атак на них составляет 5%. А чаще всего атакам подвергались госучреждения: количество атак на них выросло практически в два раза по сравнению с предыдущим кварталом.

- Злоумышленники активно распространяют шпионское ПО, направленное на кражу учетных данных. В атаках на частных лиц учетные данные составили 46% случаев от общего объема похищенной информации. Особый интерес представляют учетные данные различных VPN-сервисов, которые впоследствии продаются на теневых форумах.
- Доля шифровальщиков несколько снизилась по сравнению с IV кварталом 2021 года — с 53% до 44%. Такие изменения в определенной степени вызваны тем, что часть группировок вымогателей переходит на промышленный шпионаж без шифрования устройств. Некоторые из шифровальщиков, напротив, не присылают ключи дешифрования, нацеливаясь на разрушение инфраструктуры. Также растет число атак вайперов, которые уничтожают данные.
- ВПО продолжает попадать в официальные магазины приложений: было замечено множество, на первый взгляд, легитимных приложений, нацеленных на пользователей Android. Большинство из таких приложений являются банковскими троянами и загрузчиками, а количество скачиваний пользователями в некоторых случаях превышает сотни тысяч.
- Крупные атаки затронули IT-компании: от утечки данных пострадали такие гиганты отрасли, как Nvidia и Samsung. Также злоумышленники проводят массовые атаки на разработчиков, встраивая вредоносный код в открытые пакеты и библиотеки популярных платформ и фреймворков.

Для защиты от кибератак мы прежде всего советуем придерживаться общих рекомендаций по обеспечению личной и корпоративной кибербезопасности. Учитывая особенности I квартала, мы советуем разработчикам ПО внимательно тестировать библиотеки перед их использованием, а также контролировать защищенность и безопасную конфигурацию используемых сред разработки, проверять безопасность собственного кода. Укрепить безопасность веб-ресурсов на периметре компании можно с помощью современных средств защиты (например, web application firewalls). Чтобы предотвратить заражение устройства вредоносным ПО, мы советуем использовать песочницы, которые анализируют поведение файлов в виртуальной среде и выявляют вредоносную активность.

Как защититься обычному пользователю

1. Не экономьте на безопасности:

- используйте только лицензионное ПО;
- используйте эффективные средства антивирусной защиты на всех устройствах;
- своевременно обновляйте используемое ПО по мере выхода патчей.

2. Защищайте ваши данные:

- наиболее важные файлы храните не только на жестком диске компьютера, но и на съемных носителях, внешних жестких дисках или в облачном хранилище;
- для повседневной работы в ОС используйте учетную запись без привилегий администратора;
- используйте двухфакторную аутентификацию там, где это возможно, например для защиты электронной почты.

3. Не используйте простые пароли:

- используйте сложные пароли, состоящие из незначащих комбинаций букв, цифр и знаков, длиной не менее 8 символов. Для создания и хранения паролей можно воспользоваться менеджером паролей (защищенным хранилищем с функциями генерации новых паролей);
- не используйте один и тот же пароль для разных систем (для сайтов, электронной почты и др.);
- меняйте все пароли хотя бы раз в полгода, а лучше — каждые два-три месяца.

4. Будьте бдительны:

- проверяйте все вложения, полученные по электронной почте, с помощью антивирусного ПО;
- с осторожностью относитесь к сайтам с некорректными сертификатами и учитывайте, что введенные на них данные могут быть перехвачены злоумышленниками;
- будьте предельно внимательны при вводе учетных данных на сайтах и во время работы с онлайн-платежами;
- не переходите по ссылкам на незнакомые подозрительные ресурсы, особенно когда браузер предупреждает об опасности;
- не переходите по ссылкам из всплывающих окон, даже если рекламируемые компания или продукт вам знакомы;
- не загружайте файлы с подозрительных веб-ресурсов или из других неизвестных источников.

<u>Примеры новых приемов мошенников из обзоров СМИ.</u>

1. Названа "волшебная" фраза мошенников, заставляющая нас им поверить

Количество телефонных мошенничеств растет, а злоумышленники выдумывают все новые способы обмана, чтобы усыпить бдительность жертв и обойти сервисы безопасности. Есть фраза, с помощью которой преступникам удается довести свой замысел до конца. Она произносится в тот момент, когда мошенник забрасывает психологический крючок для того, чтобы завладеть всем вниманием собеседника. Эта фраза не примитивна, но и не так уж сложна для восприятия человеком любого возраста и уровня образования, рассказал агентству "Прайм" заслуженный юрист России Иван Соловьев.

https://1prime.ru/state_regulation/20210926/834768433.html?utm_source=yxnews&utm_medium=desktop

Эта фраза звучит так: «На вашем банковском счете зафиксирована подозрительная активность, свидетельствующая о работе мошенников».

Эта формулировка каким-то волшебным образом лишает людей бдительности и располагает к мошеннику.

В этот момент человеку стоило бы задуматься: как это заботливые "банкиры" смогли зафиксировать эту самую подозрительную активность? Но эта "волшебная" фраза почему-то отключает бдительность даже у людей, обладающих значительным жизненным опытом.

Если вы услышали знаменитую фразу про "подозрительную активность" — кладите трубку, советует юрист.

Ранее он заявил, что телефонные мошенники всегда стремятся заставить жертву играть по их сценарию. Им категорически нельзя говорить подтверждающие фразы, лучше всего заявить, что ваш разговор записан.

2. В ПФР назвали главные схемы мошенников для обмана пенсионеров

Пенсионеры все чаще становятся жертвами мошенников в силу своей доверчивости. "Российская газета" описала самые распространенные схемы мошенников, обманывающих пожилых людей. https://1prime.ru/pensions/20210920/834742285.html

Как сообщили изданию специалисты отделения ПФР по Санкт-Петербургу и Ленинградской области, всего таких схем четыре.

Первая схема — специалист на дом.

Мошенники представляются сотрудниками Пенсионного фонда и приходят к пенсионерам домой. "Иногда это делается целенаправленно — с целью выяснить, где проживают одинокие пожилые люди", — отметили в фонде.

Такие лжесотрудники предлагают пенсионерам прибавки к пенсии, перерасчет, "выгодные условия" получения пенсии и так далее. Для перевода якобы положенных россиянам выплат необходимы данные банковской карты. Именно их мошенники стараются вытянуть во время разговоров с пожилыми гражданами.

Нередко используются специальные психологические приемы: мошенники заявляют, что пенсионерам полагается крупная сумма в связи с приближающимся юбилеем либо в качестве доплаты. Но прежде чем эти деньги получить, нужно перевести определенный процент от этих денег, так называемый налог на доход.

В связи с этим отделение Пенсионного фонда напоминает, что работа с населением ведется исключительно в клиентской службе лично, в письменной форме, с помощью извещений, уведомлений и других документов либо посредством портала госуслуг и сайта ПФР.

Любые запросы от имени ПФР направляются гражданам по почте или приходят в личный кабинет на официальном сайте ПФР.

"Сотрудники ПФР не ходят по домам и не спрашивают данные банковских карт или любые другие личные данные. Поэтому ни в коем случае нельзя оставлять личные данные случайным лицам, которые звонят в квартиру и предлагают сомнительные услуги", — напоминает издание.

Вторая схема — юридическая консультация. В сети немалое количество "неофициальных сайтов Пенсионного фонда России", где транслируются недостоверные данные о пенсионных и социальных выплатах и оказываются сомнительные услуги.

Как правило, таки сайты плохо структурированы, на нем размещено много рекламы. "На помощь" посетителю такого сайта всегда приходит онлайн-чат с "пенсионным юристом", который предлагает разобраться со всеми вопросами. Переписка при этом длится недолго, человеку почти сразу предлагается оставить контактный телефон. "Если пенсионер оставляет номер, то на него звонят с предложением обратиться в "правовой центр поддержки", где человеку обещают помочь с оформлением причитающихся выплат. Такая помощь стоит недешево, но об этом потенциальная жертва "пенсионных юристов" узнает, когда уже перечисляет мошенникам деньги", — отмечает издание.

В ПФР напоминают: все услуги Пенсионного фонда предоставляются бесплатно. Для подачи любого заявления не требуется помощь посредников.

Третья схема — электронные письма. Злоумышленники присылают гражданам на электронную почту сомнительные письма, где от имени Пенсионного фонда предлагается перейти на сайт, на котором якобы можно получить причитающиеся компенсационные выплаты при переходе на сайт-подделку.

Такие данные являются фейком. ПФР не имеет к таким сайтам никакого отношения.

Еще один способ обмануть пенсионера — под видом продажи лекарственных средств. Мошенники обещают пожилым несуществующие компенсации за медикаменты и навязывают покупку дорогих препаратов, представляясь сотрудниками ПФР.

Сотрудники Пенсионного фонда никогда не предлагают людям посторонние услуги, в том числе по продаже лекарств, подчеркивают в отделении ПФР.

3. Эксперт назвал два источника информации мошенников о счетах россиян

Откуда мошенники узнают персональные данные россиян и получают сведения о состоянии их счетов, рассказал в интервью радио Sputnik руководитель проекта "КиберМосква" Григорий Пащенко. https://radiosputnik.ria.ru/20210913/moshennichestvo-1749562835.html

Службы безопасности крупных кредитных организаций практически перекрыли мошенникам путь к получению информации о клиентах после участившихся случаев обмана злоумышленниками россиян с использованием персональных данных и сведений о счетах, отметил в интервью радио Sputnik руководитель проекта "КиберМосква" Григорий Пащенко. Теперь, по его мнению, одним из основных поставщиков информации для мошенников являются микрофинансовые организации (МФО).

"Мошенники чаще всего узнают о состоянии счета человека от сотрудников микрофинансовых организаций. Крупные банки давно уже следят за тем, чтобы их операторы не сливали такую информацию. А когда МФО выдают кредиты, то у их операторов ниже социальная ответственность, они могут за небольшую плату сливать данные. Утечек из банков происходит все меньше и меньше, поскольку службы безопасности отслеживают все обращения", – объяснил эксперт.

Вторым источником сведений о россиянах для мошенников являются онлайн-магазины, считает он.

"Также злоумышленники могут узнать о состоянии счета не по выпискам из банков, а по покупкам. Они могут анализировать профиль покупок человека в интернет-магазине. Если человек в месяц закупается на 40-50 тысяч рублей, то им становится понятно, что на карте существует какая-то приличная сумма. Базы данных онлайн-магазинов являются одними из самых востребованных, по которым происходит "обзвон". По ним мошенники и работают", – уточнил Григорий Пащенко.

Чтобы защитить свои персональные и банковские данные, нужно не оставлять их на сайтах сомнительных онлайн-магазинов и компаний, соблюдая информационную гигиену, посоветовал эксперт.

4. Мошенники придумали, как выманить у россиян деньги с помощью «Госуслуг»

Россияне получают поддельные уведомления от «Госуслуг», переходят на сайт-клон и вручают деньги и личные данные в руки злоумышленников. Кибермошенники могут оформить кредит на имя жертвы или снять деньги с ее банковской карты

Атака на граждан с помощью «Госуслуг»

Кибермошенники разработали схему, чтобы вытягивать деньги и личные данные россиян от имени портала «Госуслуги». Жертва получает уведомление, в котором ей сообщают, что из-за технического сбоя произошло открепление от поликлиники. Повторная регистрация и оплата пошлины на сайте, копирующем портал «Госуслуг», приводят к утечке данных и денег преступникам, сообщило «РИА Новости». Схему выявил Сбербанк, о чем рассказал зампред правления банка **Станислав Кузнецов**.

Как работает схема

Злоумышленники в письме якобы от «Госуслуг» подчеркивают, что в условиях пандемии необходимо как можно скорее заново прикрепиться к

поликлинике. Еще один популярный вариант: «Ваш номер телефона был изменен и не может использоваться для входа». В письме жертва получает ссылку на сайт-клон, визуально повторяющем портал «Госуслуг».

Злоумышленники сразу предлагают заполнить анкету, указать поликлинику и уплатить пошлину (не превышает нескольких тысяч рублей) или, если это было сообщение об изменении номера, поменять пароль и номер телефона. Пароль и логин от личного кабинета попадает в руки недобросовестных граждан.

Возможные риски

Ситуация особенно неприятная, потому что на портале Госуслуг хранятся все персональные данные — сведения о паспорте, СНИЛС, ИНН. Иногда к профилю привязана также банковская карта, с помощью которой пользователь оплачивает налоги и пошлины. Кроме того, через «Госуслуги» мошенник может перейти в налоговую, Пенсионный фонд, портал госуслуг Москвы mos.ru.

Существует несколько возможных рисков при взломе личного кабинета на «Госуслугах». Во-первых, использование сведений с портала в базах данных позволит мошенникам максимально точно и эффективно проводить фишинговые атаки. Во-вторых, с банковской карты, привязанной к аккаунту, могут снять деньги. В-третьих, если на портале хранится скан паспорта, злоумышленник может оформить кредит на имя жертвы.

Методы борьбы

Телефонное мошенничество беспокоит не только потенциальных жертв. По словам Кузнецова, Сбербанк уже разработал программу борьбы с телефонным мошенничеством. Это позволило снизить уровень жалоб клиентов на звонки якобы сотрудников «Сбера» на 40 процентов.

В июле 2021 г. Сбербанк, а также «**Мегафон**», «**Билайн**», «**Ростелеком**» и несколько других компаний предложили новую цель для национальной программы «Цифровая экономика»: создание центра кибербезопасности для облачных госсистем и десятикратное снижение телефонного мошенничества. Компании предложили ввести регулирование IP-телефонии, блокировать звонки с подменой номера и ввести ограничения на транзит мошеннического трафика.

Банки подчеркивают, что россияне нуждаются в повышении финансовой грамотности, что позволило бы не только сохранить личные данные и деньги при столкновении с кибермошенниками, но и, например, избежать рисков при инвестировании.

5. Разработан чат-бот с искусственным интеллектом для борьбы с мошенниками

Люди не доверяют другим людям — теперь мошенники пользуются и этой маленькой особенностью человеческого характера. Подобный вывод легко можно сделать, изучив истории из первых рук. В соцсетях пользователи

во всех подробностях рассказывают, почему попались на крючок и как недоверчивость сыграла на руку именно вымогателям, а вовсе не жертве, как было бы логично предположить. https://www.cnews.ru/articles/2021-06-21_razrabotan_chatbot_s_iskusstvennym

Мошенники постоянно меняют тактику

Злоумышленники не останавливаются ни на секунду — они развиваются. Например, ведут себя, как настоящие компании, работают по обычному графику, с перерывом на обед, отдыхают в праздники, а кроме того, делают то же, что и любой другой бизнес: тщательно прорабатывают скрипты разговоров с «клиентами», учатся работать с возражениями и даже предоставляют определенный сервис. Например, присылают такси. Пенсионерку убедили получить кредит, возили на такси и рассказывали, что она поможет государству отловить мошенников. А главное, ей внушили, что близким о своих делах рассказывать нельзя ни в коем случае — нужно хранить тайну. Дочери потерпевшей даже пришлось отвести маму в полицию, чтобы та, наконец, поверила — всё это время она общалась вовсе не со строгим следователем.

А этот случай ещё более удивительный. Мошенники убедили жертву не верить словам настоящих сотрудников банка с «горячей линии», потому что они и крадут деньги! Но и это ещё не всё. Дама продолжала психологическое сопротивление и позвонила своему мужу и сестре, которые велели ей не поддаваться на посторонние уговоры. И очередной парадокс — на этот раз она не поверила собственным родственникам. А преступникам — поверила. Мастера манипуляций хорошо знают своё дело. Украденные таким образом деньги вернуть обратно не получится. Банки дают стандартный ответ: «Нет оснований для возврата средств. Мы готовы оказать любое содействие полиции по официальному запросу», — и только, ведь клиент своим руками проводил операции по счёту и снимал наличность, а банк оказывал ему услугу, как и полагается по договору. Всё честно, всё по правилам, только деньги пропали.

Кому из нас не звонил «технический директор банка» с ломающимся подростковым голосом? Но на одной и той же тактике далеко не уедешь. Приёмы скамеров меняются постоянно: публика выучила три старых, а сегодня появился один новый. Некоторым киберпреступникам сейчас даже не нужны пароли, секретные коды или CVC. Удерживая клиента на телефонной линии и не давая ему связаться с банком самостоятельно, мошенники, не спросив ни одного кода, нашли возможность обойти системы безопасности и украсть больше 220 тыс. рублей.

Кто первым встал — того и тапки

Жертвы мошенников страдают не только из-за доверия или недоверчивости, но и потому, что не могут получить помощь оперативно. В большинстве случаев попытка связаться с официальной «горячей линией» банка занимает несколько минут. Мошенники же всегда опережают официальные каналы: они за секунды переключают звонок со специалиста на

специалиста, чтобы втереться в доверие, обладают исчерпывающей информацией и кажутся очень компетентными. Это не просто специалист колл-центра, а квинтэссенция ожиданий клиента.

Некоторым пострадавшим и вовсе непонятно, куда звонить, ведь мошенники связываются с ними с номеров, имитирующих реальные телефонные номера МВД. Новый способ мошенничества обнаружили в прошлом году. МВД на своем сайте сообщило: «Номера телефонов, которые задействуются в криминальных схемах, могут быть закреплены как за банками, так и за различными подразделениями Министерства внутренних дел Российской Федерации». С сентября 2020 г. выявлено более 20 случаев реализации этой схемы. Похищено около 6,7 млн рублей.

Пандемия лишь усилила накал страстей. Весь 2020 г. хакеры выманивали данные и пароли пользователей, используя горячую тему. Например, изготовляли поддельные геокарты распространения вируса, рассылали письма, в которых обещали компенсацию пострадавшим от локдаунов. В России такие сообщения подделывались под письма с портала «Госуслуги». Уже за первые месяцы эпидемии (с февраля по март 2020 г.) количество вредоносных сайтов увеличилось на 260%, сообщили эксперты компании Trendmicro.

Центробанк в марте 2021 г. отметил еще более интересную тенденцию: атаки киберпреступников на банки особого успеха не имели, поэтому банды снова переключились с корпораций на граждан, используя интернет и смартфоны как основные каналы атак. «В 2020 г. Банк России выявил и отправил на блокировку 26,4 тыс. телефонных номеров, с которых мошенники обзванивали клиентов банков. Это почти в два раза (на 86%) больше, чем годом ранее», — пишут на сайте ЦБ.

Вызываю огонь на себя

Активным противостоянием и борьбой с мошенниками занялись все. Пользователи действовали, как обычно: предупреждали друзей и знакомых о новых схемах и заодно пытались добить мошенников юмором, выматывая их долгими разговорами по телефону. Логично: пока преступник 20 минут говорит с одним абонентом, который, к тому же, раскусил подлые намерения, другие потенциальные жертвы спят спокойно.

Этот ход мысли понравился ИТ-компаниям. Так были разработаны чат-боты, которые бросались на амбразуру скамерских писем и отвлекали мошенников бесконечно. Один только бот Re:scam отправил им больше 16 тыс. ответных сообщений. Другой бот, притворяющийся непонятливым пенсионером по имени Ленни, беседовал с преступниками по телефону. Многие так и не смогли понять, что на том конце провода «висит» вовсе не человек и раздражались, кричали и ругались — но всё тщетно. «Он отвлекает мошенников от обмана других почти 32 минуты — отлично сделано», «Ого, похоже, что злоумышленник истощен и морально, и физически», — пишут в комментариях.

Чат-бот — настоящий помощник в кризисный период

О пострадавших от мошенничества людях, которым нужна помощь прямо сейчас, подумала компания SAS. Она разработала чат-бот ViViAN. Бот запрограммирован так, чтобы чутко реагировать на разные сценарии, с которыми чаще всего сталкиваются живые операторы. Человек может спросить: «Я ответил на фишинговое письмо, что мне делать». «Кто-то пытается открыть кредитную карту на мое имя, как поступать». «Я потерял кошелек, телефон»... В ответ ViViAN задает вопросы, дает подсказки и таким образом сопровождает пользователя. Бот на базе искусственного интеллекта понимает естественную речь, анализирует, что ему написали, просматривает поток сообщений, определяя, что нужно сделать с полученной информацией, а после генерирует ответ.

Некоторые абоненты получат ответы на все свои вопросы и им хватит всего лишь одного онлайн-обращения. Для других ViViAN — это только первый шаг. «Некоторым людям потребуется помощь живого оператора. Работая с жертвами мошенничества, мы знаем, как это важно получить ценную информацию, пока ждешь разговора с реальным человеком. ViViAN может предоставить эту предварительную информацию, а затем её дополнят живые операторы, которые будут дальше сопровождать человека», — рассказывает **Ева Веласкес**, генеральный директор Центра по борьбе с хищениями персональных данных (ITRC).

ViViAN возникла в результате многолетнего партнерства между ITRC и SAS и была поддержана грантом Управления по делам жертв преступлений Министерства юстиции США. Генерация естественного языка — это технология, лежащая в основе разработки чат-бота. Она сочетает в себе три особые возможности для создания интерактивных чат-ботов, таких как ViViAN, которые понимают и взаимодействуют с человеческим языком.

«Мошенники буквально не дремлют. Вы можете узнать, что стали их жертвой в ночное время. Но теперь есть возможность задать вопрос или получить оперативную помощь ViViAN — днем и ночью», — комментирует Ева Веласкес. Если люди слабо доверяют друг другу и вынуждены подолгу ждать ответов от официальных источников, то, возможно, неподкупный и независимый чат-бот, отвечающий мгновенно, станет хорошим подспорьем в нашей общей борьбе против мошенников.

6. «Гарант» сообщает: Личные финансы: что нового в сфере защиты граждан от действий мошенников?

Одновременно с активным развитием цифровых технологий возрастают и возможности использования этих технологий для совершения противоправных деяний. Причем мошенники постоянно совершенствуются, изобретают новые схемы, применяют самые современные психологические приемы.

Так, в последнее время широкое распространение получило мошенничество с использованием метода социальной инженерии, когда человек сам передает мошенникам номера платежных карт, коды, пароли. В

связи с этим недавно Минфин разработал поправки в законодательство, которые позволят ускорить раскрываемость таких схем.

Потерять деньги граждане рискуют и из-за переводов в адрес нелегальных структур (незаконных онлайн-казино, организаторов финансовых пирамид и др.). Поэтому за банковскими транзакциями физлиц начнут следить еще внимательнее. В начале сентября 2021 г. Центробанк определил критерии, по которым банки смогут выявлять платежные карты и электронные кошельки, используемые теневым бизнесом.

И еще одно нововведение, которое направлено на защиту прав потребителей финансовых услуг, - с 10 сентября 2021 г. финансовые организации при заключении договоров с физлицами обязаны письменно информировать их о возможных рисках. Подробно об этом мы рассказывали ранее.

«Лаборатория Касперского» разработала программы по информационной безопасности для средней и старшей школы

https://www.kaspersky.ru/about/press-releases/2021_laboratoriya-kasperskogo-razrabotala-programmy-po-informacionnoj-bezopasnosti-dlya-srednej-i-starshej-shkoly

Сайт компании 2 сентября 2021 г. сообщил:

На открытом Августовском педагогическом совете в Москве «Лаборатория Касперского» представила образовательную программу по информационной безопасности для учащихся 7-9 и 10-11 классов. Материалы смогут использовать на своих уроках учителя информатики.

Курс для 7-9 классов состоит из шести модулей и знакомит учеников с основами защиты информации в сети, персональных данных и личных финансов, безопасности мобильных и IoT-устройств. В процессе обучения школьники узнают об основных угрозах в интернете, в том числе фишинге, вредоносных программах, онлайн-травле, и о том, как им противостоять. Курс для 10-11 классов предполагает более глубокое погружение в тему информационной безопасности и состоит из четырёх модулей. Программа включает изучение самого понятия киберпреступности, способов защиты данных с использованием различных шифров и алгоритмов, основ безопасности ПО, а также законодательных норм в области кибербезопасности и регулирования интернета.

Для учителей подготовлен специальный курс повышения квалификации «Обеспечение комплексной защиты информационного пространства подростка в современных условиях». Он позволяет освоить методику преподавания программ, разработанных «Лабораторией Касперского».

«Мы давно поддерживаем развитие школьного образования в области информационной безопасности, в частности участвовали в подготовке обновлённой версии учебников по информатике. Наш новый шаг в этом направлении — разработка учебных модулей, пошаговой программы для средней и старшей школы. В курсе для 7-9 классов мы сосредоточились на

том, чтобы помочь развить критическое мышление, выработать навыки безопасного общения в сети, научить распознавать наиболее распространённые угрозы. Курс же для старшей школы предпрофессиональный. В нём идёт речь об информационной безопасности как об отрасли, рассказывается, какие задачи и проблемы стоят перед индустрией и как они решаются. Мы надеемся, что уже в этом учебном году наш спецкурс появится в расписании значительного количества столичных школ, как это рекомендует Департамент образования и науки города Москвы», — комментирует Вениамин Гинодман, советник генерального директора «Лаборатории Касперского» по образовательным проектам.