СТРАТЕГИЯ ПОВЫШЕНИЯ ФИНАНСОВОЙ ГРАМОТНОСТИ
В РОССИЙСКОЙ ФЕДЕРАЦИИ НА 2017-2023 ГОДЫ

# ФИНАНСОВОЕ КОНСУЛЬТИРОВАНИЕ

МИНИСТЕРСТВО ФИНАНСОВ
Российской Федерации

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

# Кибербезопасность личных средств и новые цифровые платформы и инструменты.

Наша лекция будет посвящена рассмотрению основных видов кибератак и способов обеспечения своей безопасности в киберпространстве. Также расскажу о типовых схемах воздействия методов социальной инженерии и об инструментах анализа источников информации о человеке.

В качестве **основных угроз кибератак** можно выделить:

**1) Взлом учетной записи, аккаунта**. Здесь последствия могут быть разными. От вашего имени будет осуществляться спам-рассылка или отправка мошеннических писем, другие кибер-атаки, включая несанкционированный доступ к корпоративным системам и базам данных.

**2) Шантаж** с целью получения каких-либо услуг или денежного вознаграждения.

**3) Продажа ваших данных.**

**4) Финансовые махинации** от вашего имени или с вашими счетами и цифровыми кошельками, если украденная информация позволяет это осуществить.

Первым делом, чтобы себя обезопасить в киберпространстве, необходимо **соблюдать базовые правила парольной политики**. Прежде всего, для каждого интернет-ресурса, приложения, прикладной системы нужно использовать разные пароли. Это неудобно — столько всего запоминать, но это существенно снижает риски взлома. **Хороший пароль должен состоять минимум из 8 знаков, включая буквы, цифры и специальные символы**. Это обусловлено технологическими возможностями атакующих систем. Так, например, для подбора пароля из 7 знаков достаточно 2 секунд, из 8 — 2 минут, из 10 — потребуется 3 дня. Пока мошенник будет подбирать пароль, система безопасности распознает атаку и сможет ее предотвратить. Также важно, чтобы пароль не содержал слова из словарей, персональных данных, которые легко

узнать, например, фамилию мамы или дату вашего рождения. Специалисты **рекомендуют подбирать сложные пароли, но которые легко будет запомнить именно вам**. Например, состоящие из первых букв припева любимой песни.

Если вам кажется, что **вашу почту или аккаунт в социальных сетях, в мессенджере взломали, выполните ряд действий** для минимизации потерь:

**1. Постарайтесь сменить пароль.** Если не получается, а такое бывает, когда злоумышленник заблокировал эту опцию, то обратитесь в службу поддержки соответствующего почтового сервиса или социальной сети за восстановлением аккаунта.

**2. Обязательно предупредите свои контакты о произошедшем.**

3. Затем, **войдя в аккаунт, проверьте его настройки**. Там тоже могут быть изменения. Например, настроена пересылка всех писем на другой адрес или изменен адрес для ответа на ваши письма.

4. И **обязательно установите или обновите антивирусную программу** на вашем устройстве. Она поможет выявить вредоносные программы и закладки, которые могут быть ранее установлены злоумышленником.

Для защиты персонального компьютера, планшета, мобильного телефона целесообразно использовать разные методы и средства-помощники. Чтобы защитить свои учетные записи, логины и пароли, **рекомендуется использовать** не однофакторную аутентификацию, когда вы только вводите пароль, а **двухфакторную или многофакторную**, когда кроме пароля еще вводите код, поступающий по СМС. Или когда **помимо пароля запрашиваются еще и биометрические данные**, например, голос или отпечаток пальца. Также сохранить и защитить пароли помогут специальные приложения и сервисы, например: **менеджер паролей.**

Для более **глобальной защиты устройств и систем используются антивирусные приложения, программы обнаружения и помещения в карантин подозрительных писем и сообщений**. Важно устанавливать регулярные обновления этих приложений. Поскольку киберпреступники постоянно разрабатывают новые варианты и методы атак. Для

конфиденциальной информации и документов, содержащих особо важные сведения, используются **технологии криптографической защиты, цифровые подписи** и т.п. Также не стоит забывать про **защиту мобильный устройств**, поскольку их кража более вероятна, чем настольного компьютера.

**Кибератаки и компьютерные атаки можно условно разделить на несколько типов**.

1) Наиболее распространенными среди обычных пользователей являются **мошеннические группы и аккаунты в социальных сетях**.

2) Часто люди попадают на **поддельные или мошеннические сайты**.

3) Далее следуют **фишинговые атаки** через электронную почту, мессенджеры и СМС.

4) **Программы-вымогатели** являются также довольно-распространенным видом компьютерных атак. Однако они в основном нацелены на бизнес, а не на физических лиц. Они блокируют работу устройства или какого-то важного приложения и требуют выкуп для разблокировки. Также могут требовать вознаграждение за нераскрытие вашей личной информации, которая была незаконно добыта подобным путем.

5) Другим типом кибератак являются **мобильные приложения с вредоносным кодом или фишинговыми формами**, которые предлагаются к установке.

6) Кроме того, часто наблюдается **реализация разных мошеннических схем на маркетплейсах**, в приложениях знакомств или компьютерных играх. Подавляющее большинство из них реализуется методами социальной инженерии, которые рассмотрим чуть позднее.

В киберпространстве выделяют **три основных способа сбора данных банковских карт и счетов**:

**1. Использование поддельных интернет-магазинов и сбор средств на благотворительность**, где человек довольно быстро и эмоционально принимает решение о перечислении средств.

**2. Перехват информации через зараженные страницы официальных магазинов или устройства пользователя**. Например, с помощью банковского троянского коня. Который собирает и передает информацию злоумышленнику при вводе банковских реквизитов на собственном ноутбуке.

**3.** Также может быть **взломан сайт интернет-магазина** и украдены данные оттуда.

В качестве **методов защиты** можно предложить **использовать виртуальные банковские карты для онлайн-операций и регулярно их перевыпускать**. Примерно раз в год. **Установить лимит на карты, проверять корректность платежной операции**. Также рекомендуется перед одобрением платежа внимательно **перепроверить платежную форму и адрес сайта,** на котором осуществляется операция.

В подавляющем большинстве случаев атаки на физических лиц совершается **с помощью методов социальной инженерии**, которая заключается в том, чтобы **обманным путем вынудить человека добровольно предоставить доступ к компьютеру, мобильному телефону, платежной карте или передать какие-либо данные**. Важно отметить, что, как правило, воздействие идет через доверие или провоцирование ярких эмоций. Например, знакомый попал в беду или служба безопасности просит срочно сообщить пароль и логин, чтобы предотвратить утечку информации.

- Часто атака социальной инженерии целенаправленно готовится. Злоумышленник изучает жертву, собирает о ней необходимую информацию и определяет оптимальный метод атаки.
- Затем переходит к обработке. Например, входит в доверительный контакт с жертвой. Представляется генеральным директором компании, которого человек может знать заочно. Или менеджером какой-либо знаменитости.
- Вы становитесь заинтересованы в данном общении, начинаете доверять и попадаете в ловушку.

- Затем начинается атака, в ходе которой под разными предлогами, просьбами (срочными и не очень) добывается информация. Это может быть как персональные данные, например: адрес проживания, паспортные данные или номер кредитной карты, так и информация, составляющая коммерческую тайну.
- И последний этап атаки — сокрытие ее следов и максимальное сохранение доверия, чтобы жертва не распознала, что произошло незаконное завладение информацией.

Другая довольно распространенная схема атаки на компьютер и корпоративные сети — это **подбрасывание флешки**, например, около рабочего места или входа в офис. На ней может быть завлекающее название: «отчет 2023» или «личные фото 2023». Такую информацию непременно захочется посмотреть, и вы вставите флешку в компьютер. А там будет вредоносная программа или троянский конь.

Другой вариант заражения — **это просьба коллеги распечатать вас документ**, поскольку у него что-то там не работает.

В ходе подготовки к индивидуальной атаке мошенник основательно исследует информацию о жертве из разных открытых интернет-источников. Начиная с обычного поискового запроса в браузере, анализом страниц в социальных сетях и заканчивая применением специальных мониторинговых и аналитических программ и сервисов. Мы, активно пользуясь социальными сетями, мессенджерами, оставляем о себе длинный **пользовательский след**, анализ которого позволит злоумышленнику узнать о нас многое. Например, с кем мы дружим, где гуляем, что едим, каковы наши интересы, проблемы, место работы и .т.д. Вся **эта информация поможет преступнику сделать вас жертвой кибер-атаки.**

Итак, в качестве заключения хочу еще раз перечислить основные действия, которые помогут вам защитить себя, свои данные и деньги в киберпространстве:

**1.** Остановитесь и подумайте, прежде чем нажать на ссылку. Не торопитесь, даже если вас об этом очень просят.

**2.** Создавайте сложные пароли, используйте многофакторную аутентификацию.

**3.** В ходе онлайн-покупок проверяйте безопасность транзакций, платежные реквизиты, ресурс, где вы производите оплату.

**4.** Используйте для этого виртуальные банковские карты.

**5.** Присмотритесь к программам-помощникам, которые могут защитить вас от мошенников.

**6.** И последнее — задумайтесь о своем цифровом следе в сети.

МИНИСТЕРСТВО ФИНАНСОВ
Российской Федерации

ФИНАНСОВЫЙ УНИВЕРСИТЕТ
ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ