ТРЕНИНГ ОБЩЕСТВЕННЫХ ЭКСПЕРТОВ ПАЦИЕНТСКОГО ДВИЖЕНИЯ

Цифровая безопасность: защита личных данных в онлайн пространстве

Куличкин Артём Александрович

И.о. Директор по информационной безопасности ДЗО «СОГАЗ».

CEH, CISA, CISM, CISO.

Москва, 27 ноября – 1 декабря 2024

https://congress-vsp.ru/xv/

Введение

- Информационная безопасность – это не только для специалистов. Каждый день мы сталкиваемся с рисками в интернете: от фишинга до кражи данных. Эта лекция поможет нам понять основные угрозы и научиться защищаться. Мы рассмотрим простые, но эффективные методы обеспечения безопасности вашей информации.

Угрозы

- **Фишинг и мошенничество**
- **Вирусы и вредоносные программы**
- **Безопасность мобильных устройств**
- **Онлайн-банкинг и платежи**
- **Слабые пароли**
- **Социальные сети и конфиденциальность**
- **И многое другое…**

Как же нам изменить ситуацию?

Фишинг и мошенничество

- Будьте осторожны с подозрительными ссылками и электронными письмами
- Проверяйте отправителя сообщения перед тем, как открывать его
- Не переходите по ссылкам из неизвестных источников
- Никогда не передавайте личные данные по электронной почте или телефону, если вы не уверены в источнике запроса
- Обращайте внимание на орфографические ошибки и несоответствия в дизайне

Социальная инженерия работает по-разному:

звонки по рабочему или мобильному телефону

сообщения в мессенджерах и смс

сообщения по электронной почте

с помощью оставленных носителей информации

Злоумышленники рассчитывают на замешательство человека, а также быстрое и необдуманное принятие решения.

Всегда будьте внимательны при общении с незнакомым человеком!

Массовый обзвон

Этот вид атак применяется по телефону и проходит по заранее подготовленному сценарию.

В результате звонка цель должна предоставить личную информацию (например, ФИО, занимаемую должность, данные кредитной карты или номер паспорта) или совершить какие-либо действия (переход по ссылке, ввод учетных данных
или загрузку зараженного файла).

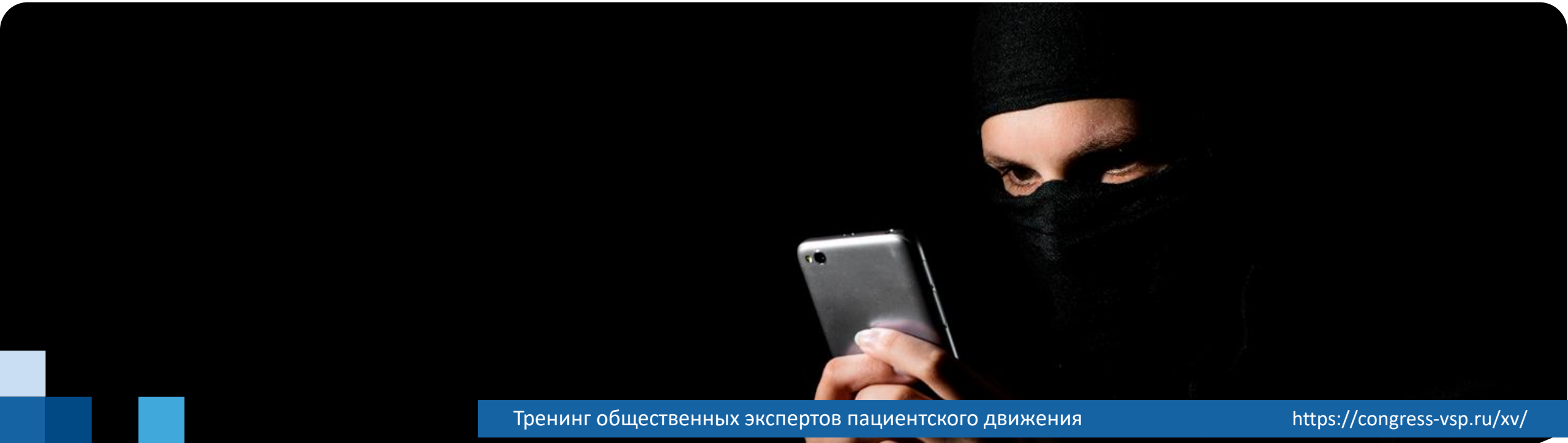
Никогда ни при каких обстоятельствах
не сообщайте личные данные людям, позвонившим с неизвестного номера!

Лучше самостоятельно перезвонить
в отделение банка или по официальному телефону организации, работником которой представился звонящий.

Телефонное мошенничество

Злоумышленник может позвонить и представиться специалистом технической поддержки, проводящим тестирование или настройку программного обеспечения.

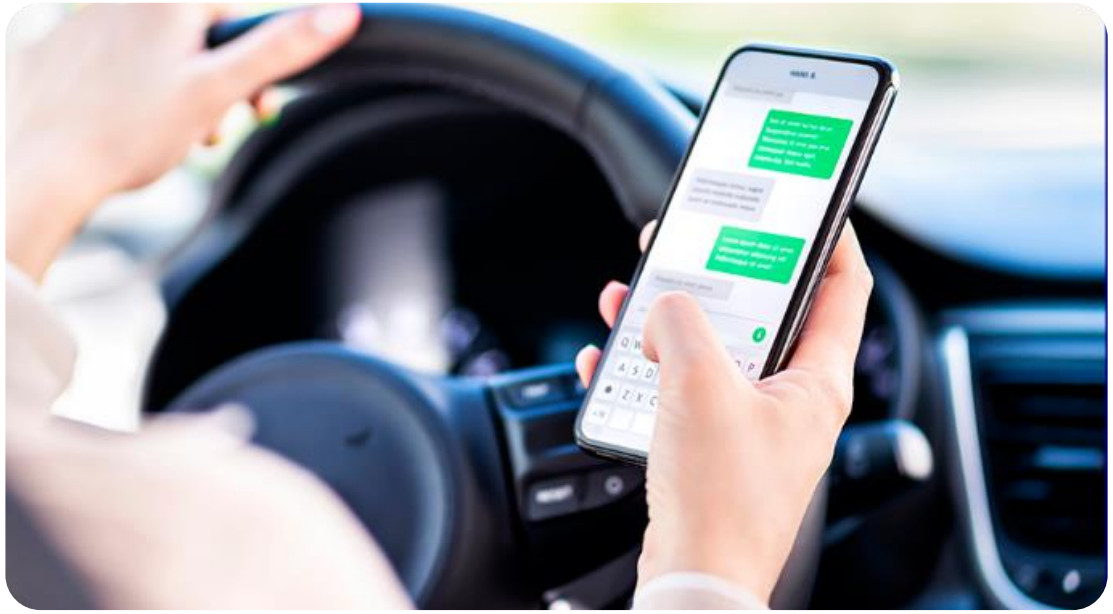
В процессе общения человек (жертва) выполняет команды, которые позволяют злоумышленнику запустить вредоносное программное обеспечение или совершить мошеннические действия.



Смс-фишинг

Для проведения фишинговой атаки используются смс,
а не электронная почта.

Принцип действия такой же, как и при осуществлении фишинговых атак — заставить человека перейти по вредоносной ссылке, завлекая выгодным предложением.



Зараженный съемный носитель

Злоумышленник подбрасывает зараженную флешку или CD/DVD туда, где носитель информации может быть легко найден человеком (коридор, лифт, парковка).

После подключения носителя происходит заражение компьютера сотрудника.

Обратная социальная инженерия

Цель обратной социальной инженерии — заставить человека самого обратиться к злоумышленнику за «помощью».

Например, злоумышленник может прислать объявление вида:

«Если возникли проблемы с компьютером, позвоните по номеру 8 (800) ******* »,

после чего вызвать неполадки на компьютере.

Ложные Wi-Fi сети

Злоумышленники могут использовать поддельные беспроводные точки доступа для сбора вашей информации.

Для этого они создают в общественном месте ложную точку доступа с примерным названием «Free Wi-Fi».

После установки подключения к Wi-Fi злоумышленник осуществляет перехват данных между устройством жертвы и поддельной точкой доступа с целью осуществления дальнейших злонамеренных и вредоносных действий.

Не подключайтесь без крайней необходимости к публичному Wi-Fi, так как в случае успешной атаки в руки злоумышленника может попасть конфиденциальная информация, такая как электронная почта, учетные записи, пароль, номер кредитной карты и др.

Атака, которая может заразить компьютер или телефон

Фишинг — вид интернет-мошенничества, цель которого — получение доступа к конфиденциальным данным пользователя.

Пример:

Злоумышленник может под видом контрагента или банка отправить на e-mail жертвы письмо с вложением, просьбой перейти по ссылке (или ввести данные). После этого происходит заражение компьютера.

Разновидности фишинга

Почтовый фишинг
(Email phishing)

Телефонный фишинг
(Vishing)

Смс-фишинг
(Smishing)

Почтовый фишинг // Письма со сценарием

Злоумышленник выдает себя
за легитимную личность
или организацию, отправляя массовые
электронные письма
на случайные адреса электронной почты.

Такие письма содержат угрозы
или побуждения к действию (например,
сообщение получателю,
что его личный счет был взломан,
а потому он должен немедленно ответить).

Цель заключается в том, чтобы
срочностью спровоцировать
человека
на необдуманное, но вполне
определенное действие.

Например, нажать на вредоносную
ссылку, которая ведет на
поддельную страницу авторизации
или открыть зараженный файл.

Почтовый фишинг // Целевой фишинг

Такие письма часто более персонализированы и заставляют жертву поверить, что они знают отправителя.

Злоумышленник отправляет вредоносные электронные письма определенным лицам информацию о которых он нашёл информацию в открытых источниках.

Почтовый фишинг // Целевой фишинг

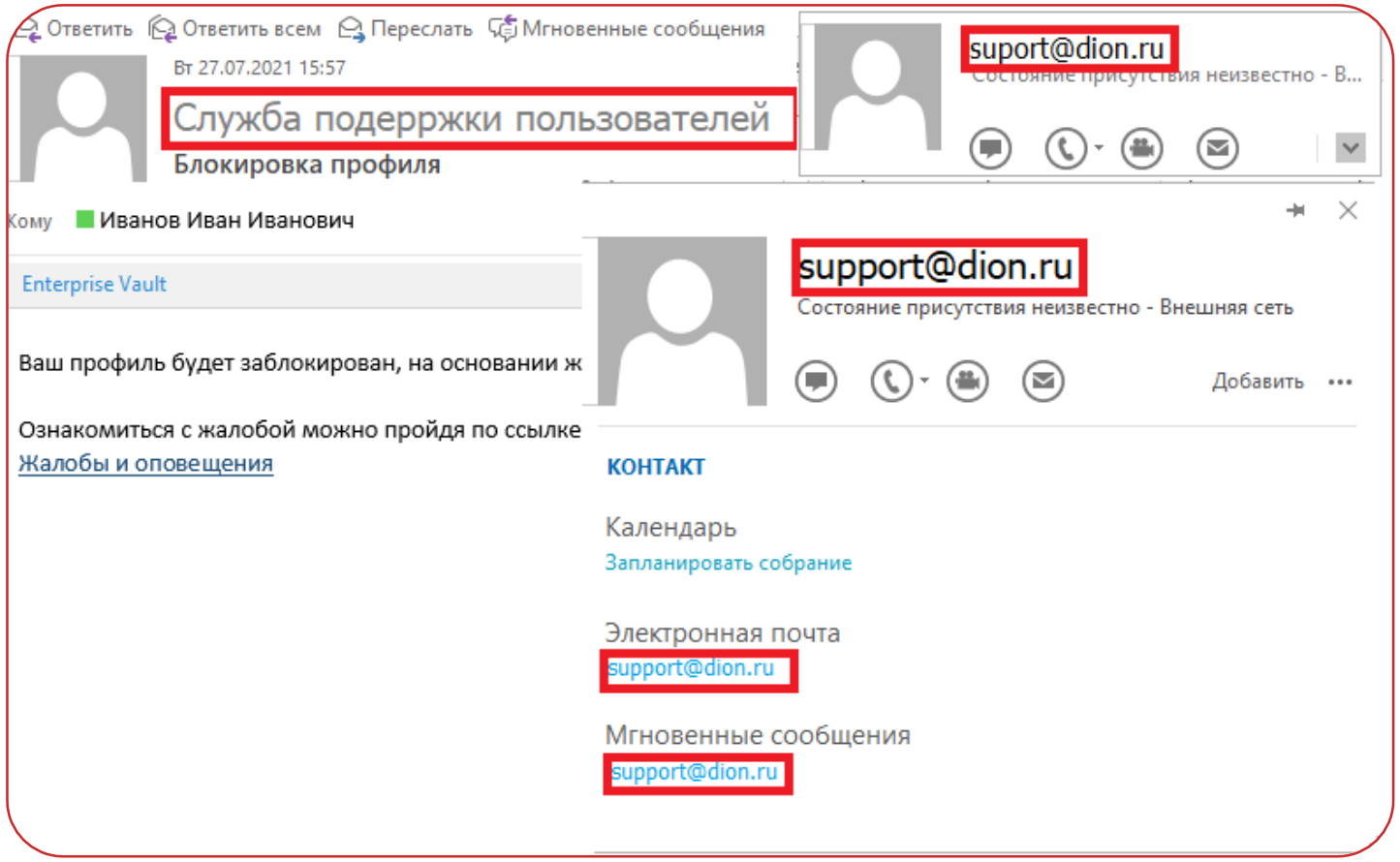
Признаки мошеннического письма

Примеры ↘

- Незнакомый отправитель
- Подозрительное содержание
- Речевые ошибки
- Наличие ссылок и переходов на другие сайты или сервисы

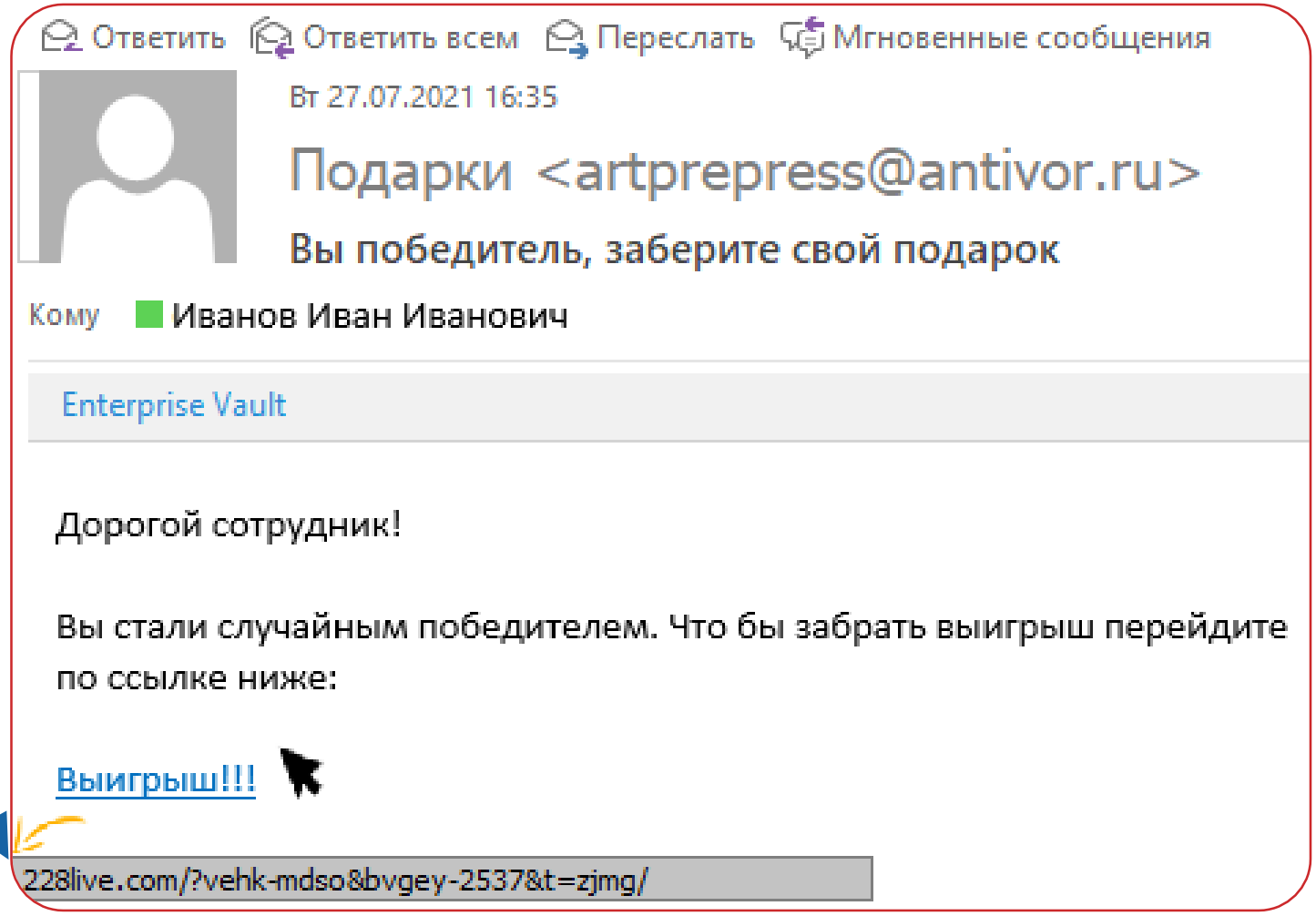
Незнакомый отправитель

Внимательно посмотрите на адрес отправителя. При фишинговых атаках email вам незнаком или указан с явной ошибкой в известном домене (после @).



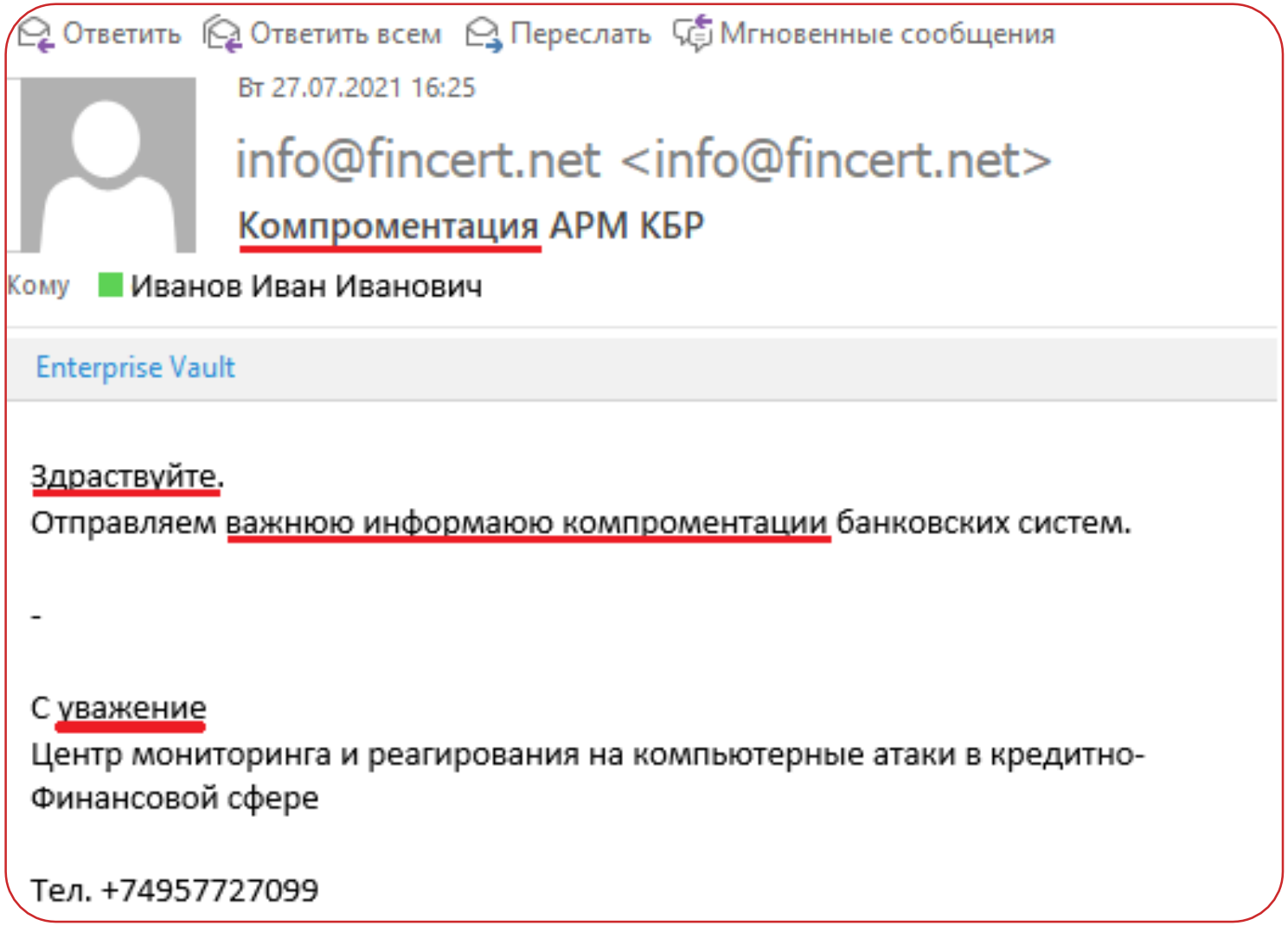
Наличие ссылок и переходов на другие сайты

Вредоносные ссылки могут быть спрятаны в разных местах: кнопки, текст, картинки и т. д.



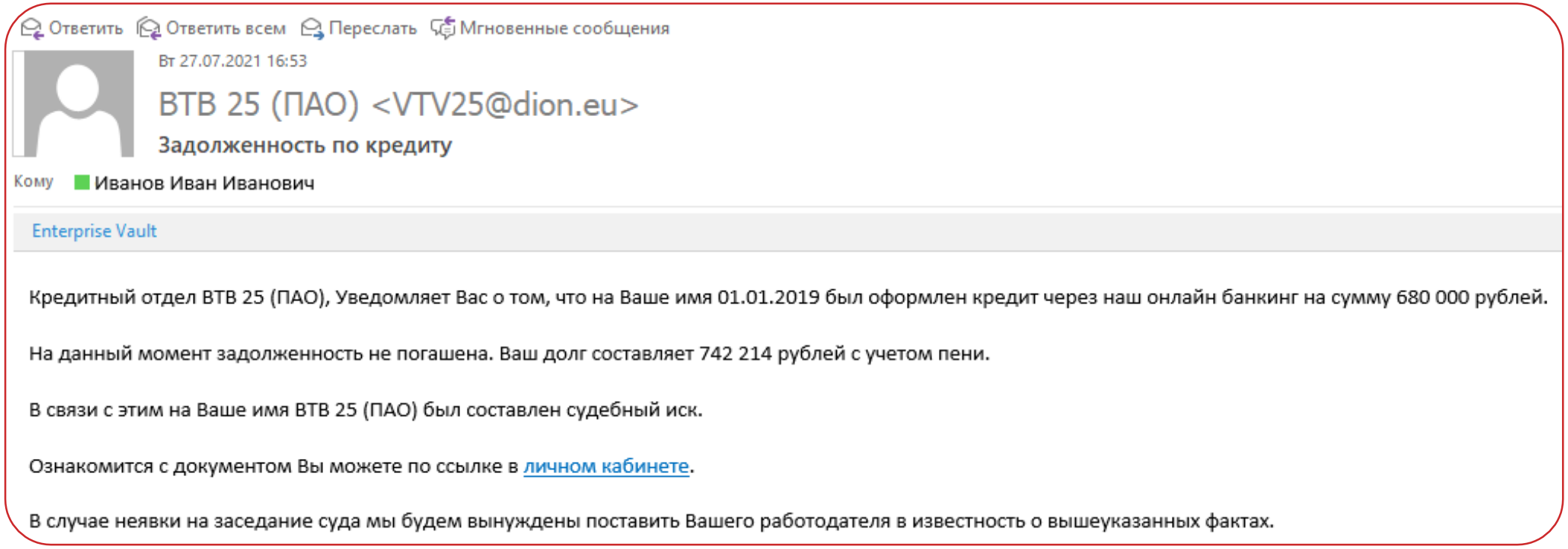
Наличие ссылок и переходов на другие сайты

В письме и теме письма присутствуют грамматические и/или речевые ошибки.



Подозрительное содержание

Вы не ожидали подобное письмо
или оно содержит угрозы, призывы к действию,
желание получить какую-либо выгоду
или информацию,
не соответствующую вашим ожиданиям.



Ответить Ответить всем Переслать Мгновенные сообщения

Вт 27.07.2021 16:53

ВТВ 25 (ПАО) <VTV25@dion.eu>

Задолженность по кредиту

Кому Иванов Иван Иванович

Enterprise Vault

Кредитный отдел ВТВ 25 (ПАО), Уведомляет Вас о том, что на Ваше имя 01.01.2019 был оформлен кредит через наш онлайн банкинг на сумму 680 000 рублей.

На данный момент задолженность не погашена. Ваш долг составляет 742 214 рублей с учетом пени.

В связи с этим на Ваше имя ВТВ 25 (ПАО) был составлен судебный иск.

Ознакомится с документом Вы можете по ссылке в личном кабинете.

В случае неявки на заседание суда мы будем вынуждены поставить Вашего работодателя в известность о вышеуказанных фактах.

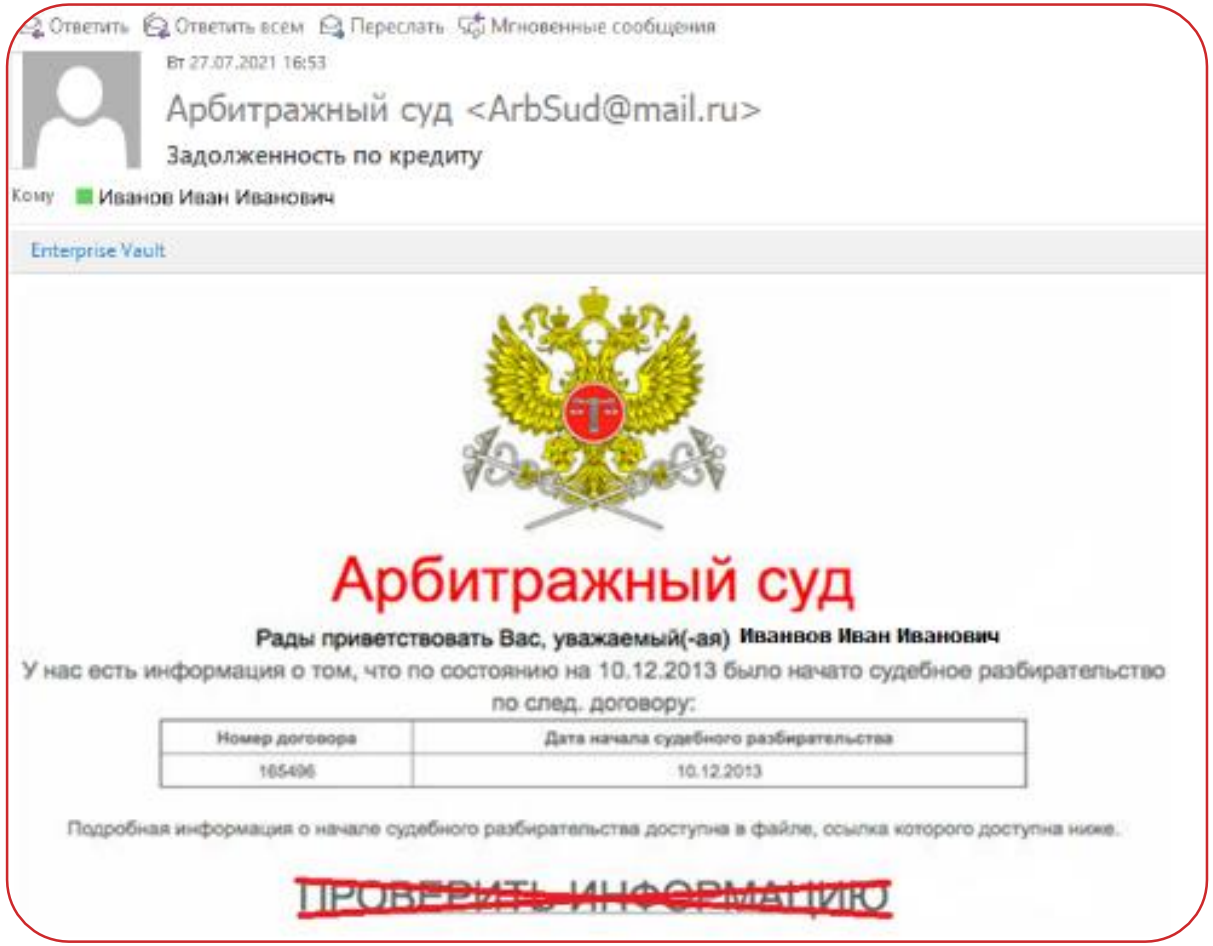
Что делать?

Что делать с мошенническим письмом?

Что делать?

Не переходите по ссылкам,
не нажимайте кнопки в письме

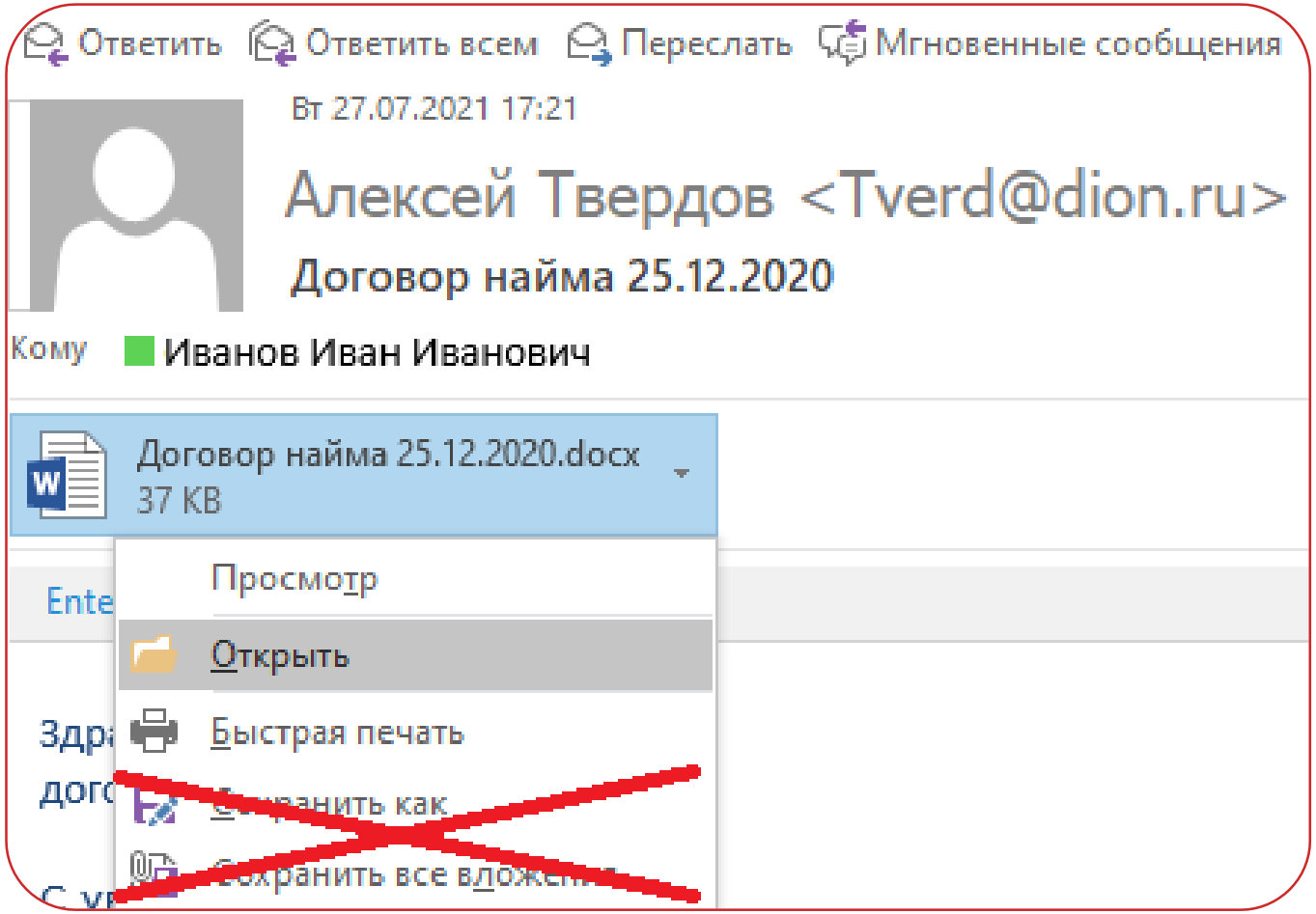
Ни при каких обстоятельствах не совершайте данные действия!



Что делать?

Не открывайте и не просматривайте вложения в письме

Ни при каких обстоятельствах не совершайте данные действия!



Что делать?

Ни при каких обстоятельствах не совершайте данные действия!

Не вводите никаких данных в полях, если вы случайно перешли по ссылке

Что делать?

Ни при каких обстоятельствах не совершайте данные действия!

Не отвечайте на письмо и самостоятельно никому не пересылайте его

Вирусы и вредоносные программы

- Установите надежный антивирус и регулярно обновляйте его.
- Будьте осторожны при скачивании файлов из интернета.
- Не открывайте вложения от незнакомых отправителей.
- Регулярно сканируйте компьютер на наличие вирусов.
- Создавайте резервные копии важных данных.

Безопасность мобильных устройств

- Установите надежный пароль и PIN-код на вашем смартфоне.
- Включите функцию автоматического блокирования экрана.
- Используйте функцию поиска устройства в случае его потери или кражи.
- Не скачивайте приложения из ненадежных источников.
- Регулярно обновляйте программное обеспечение вашего устройства.

Онлайн-банкинг и платежи

- Используйте только безопасные веб-сайты для онлайн-банкинга и покупок.
- Обращайте внимание на адрес веб-сайта (https://).
- Никогда не используйте общедоступные компьютеры для онлайн-банкинга.
- Проверяйте выписки по банковским счетам регулярно.
- Не храните данные банковских карт, крипто кошельков и тд.

Пароли: основа безопасности

- Ваш пароль длинный?
- Ваш пароль трудно угадать?
- Разнообразен ли состав символов в вашем пароле?
- Есть ли в вашем пароле очевидные подстановки символов?
- Есть ли в вашем пароле необычные сочетания слов?
- Сможете ли вы запомнить свой пароль?
- Пользовались ли вы этим паролем раньше?
- Используете ли вы правило, которое трудно разгадать компьютеру?

Пароли: основа безопасности

Кодовые фразы

Пример кодовой фразы – «коровА!жгИ»алыЙ№репА;» (здесь использованы слова «корова», «жги», «алый» и «репа»).

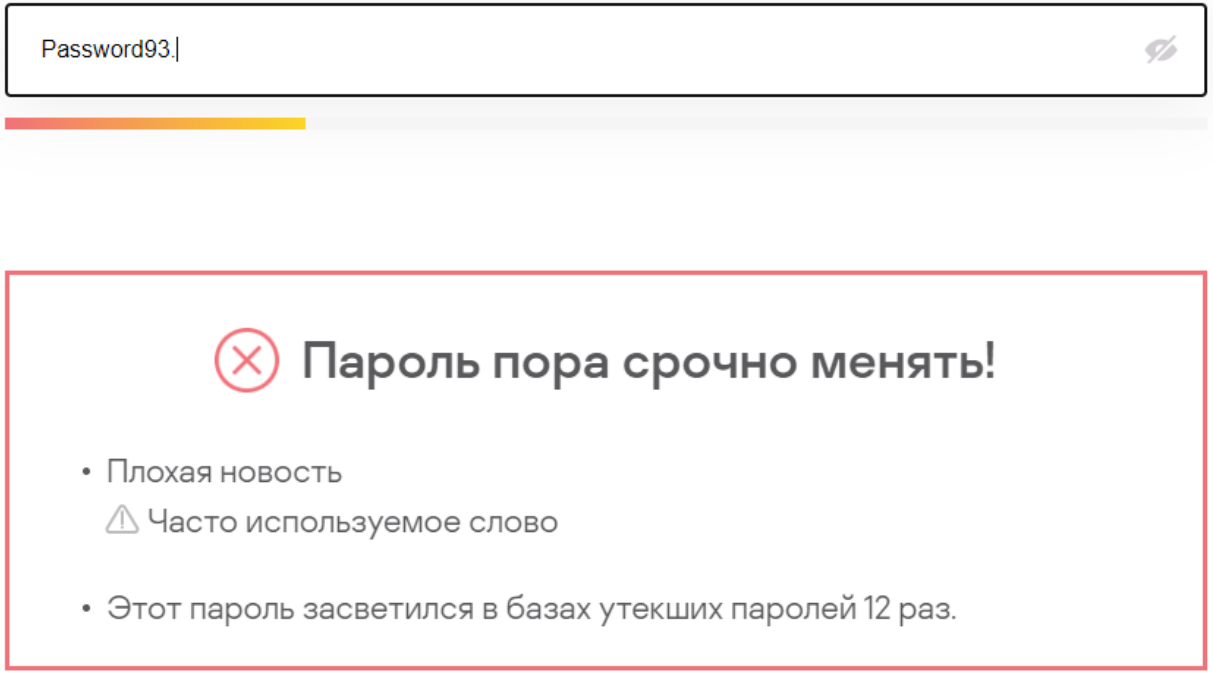
Цепочки случайных символов

Пример цепочки случайных символов: «f2a_+Vm3cV*j».

Пароли: основа безопасности

- Используйте уникальные пароли для каждого аккаунта.
- Создавайте сложные пароли: длинные, с использованием разных регистров, цифр и символов.
- Используйте менеджер паролей для хранения и управления паролями, например: KeePass.
- Не используйте личную информацию в паролях.
- Регулярно меняйте пароли, особенно для важных аккаунтов.

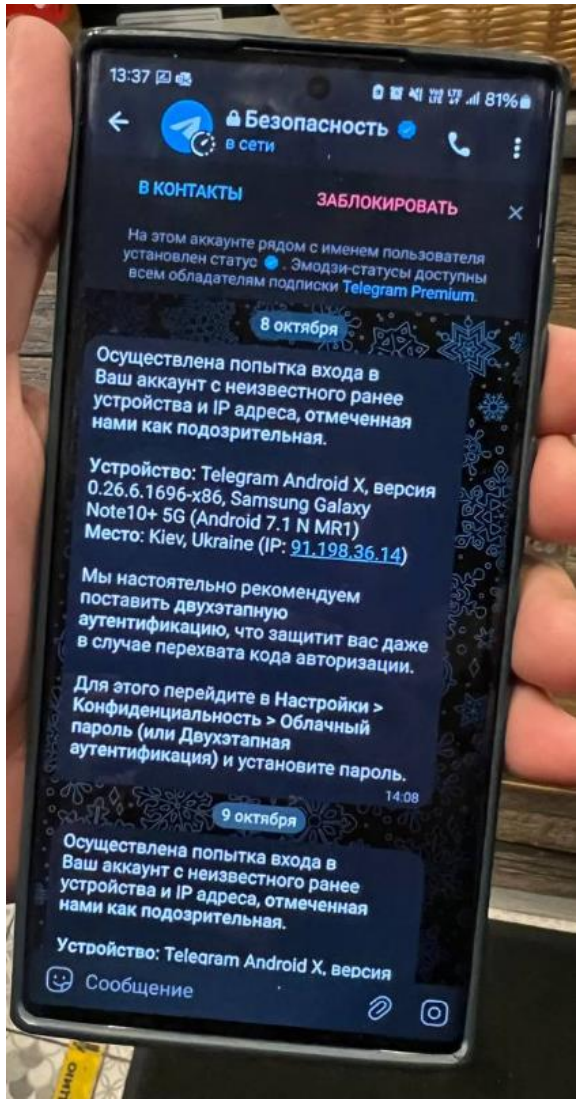
Проверка пароля на надежность и сложность онлайн | Kaspersky

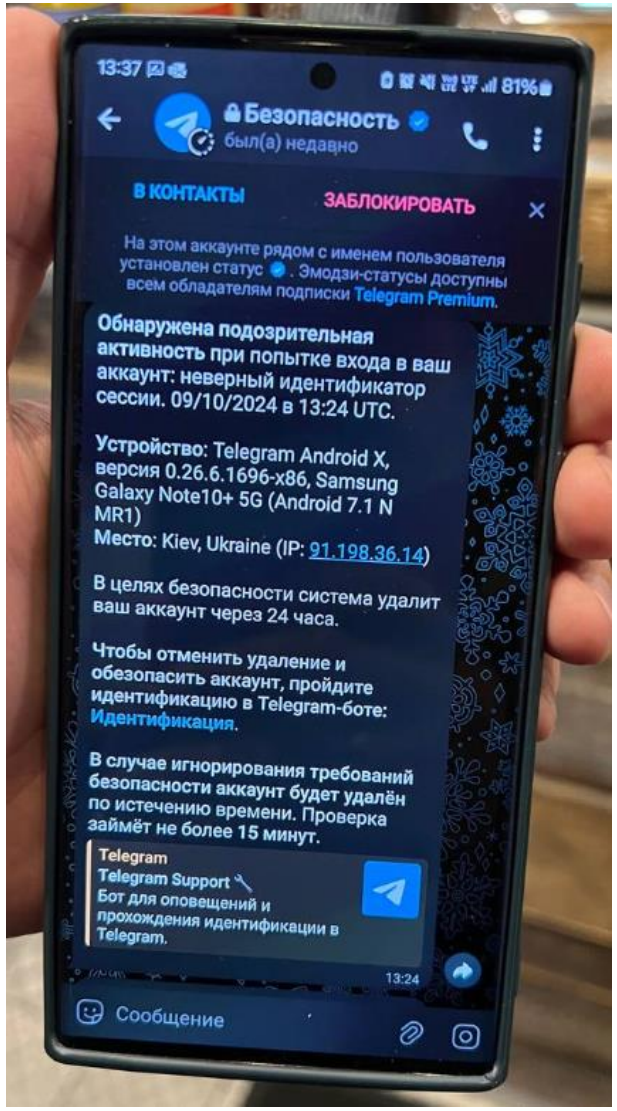


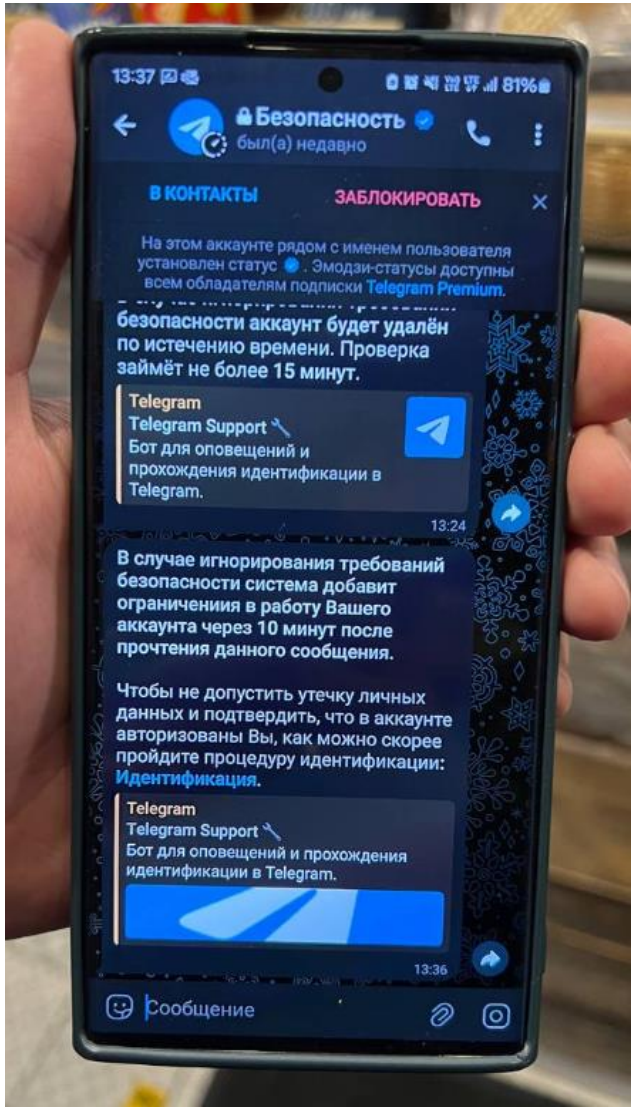
Социальные сети и конфиденциальность

- Будьте осторожны с информацией, которую вы публикуете в социальных сетях
- Включить везде 2FA где это возможно
- Запретите звонки незнакомым
- Регулярно проверяйте ваши устройства в настройках
- Настройте параметры конфиденциальности в социальных сетях
- Не добавляйте в друзья незнакомых людей
- Не делитесь личной информацией в социальных сетях
- Будьте внимательны к мошенническим схемам в социальных сетях

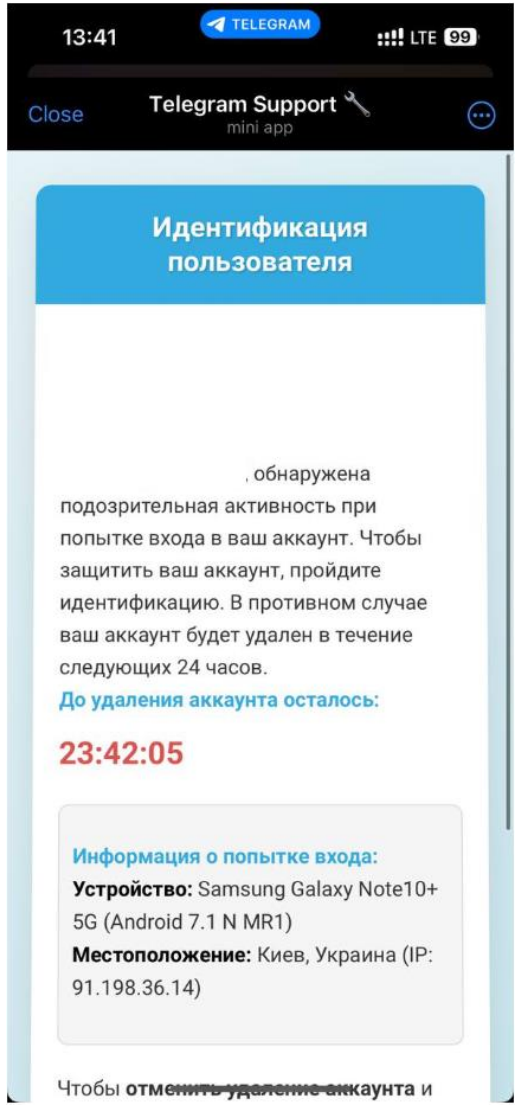
Социальные сети и конфиденциальность

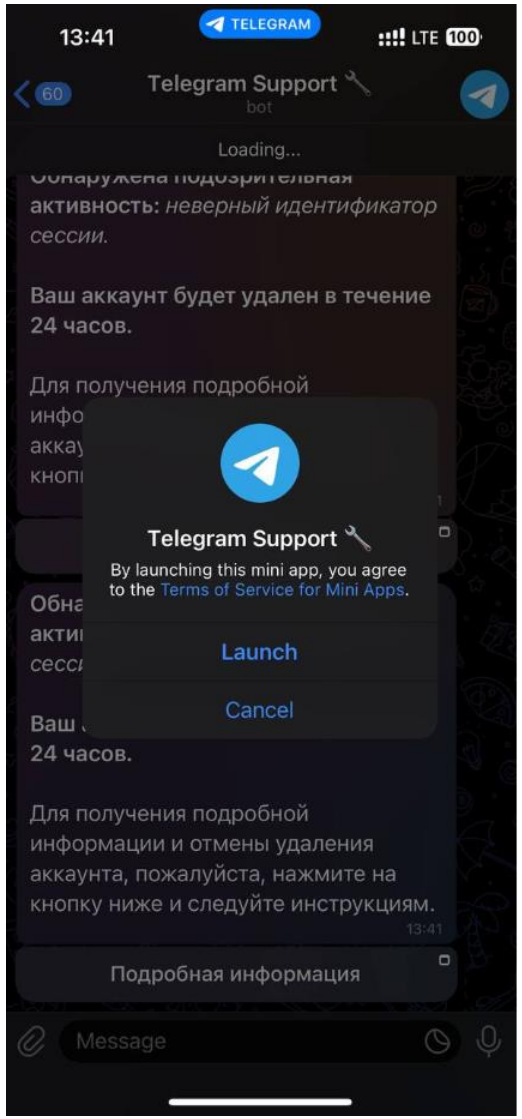


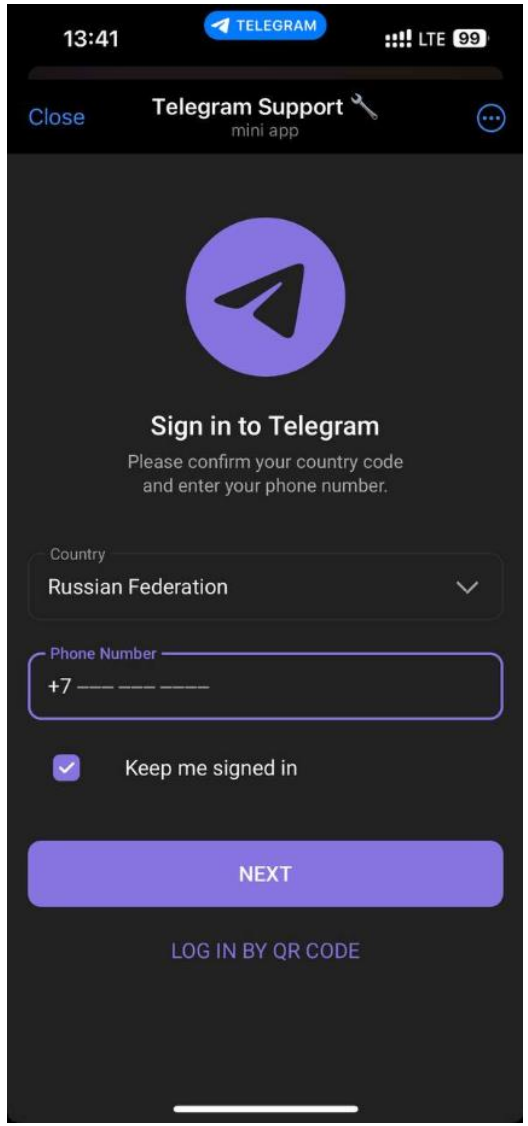




Социальные сети и конфиденциальность







Резервное копирование данных

- Не использовать облачные хранилища для резервного копирования данных
- Создавайте резервные копии важных данных регулярно
- Храните резервные копии в безопасном месте
- Проверяйте работоспособность резервных копий периодически
- Защитите резервные копии паролем

Заключение

- Информационная безопасность – это непрерывный процесс. Следуя этим советам, вы значительно повысите уровень защиты вашей личной информации и сведете к минимуму риски киберугроз. Помните, что бдительность и осторожность – ваши лучшие союзники в цифровом мире. Оставайтесь в безопасности!

БЛАГОДАРЮ ЗА ВНИМАНИЕ!

ТРЕНИНГ ОБЩЕСТВЕННЫХ ЭКСПЕРТОВ ПАЦИЕНТСКОГО ДВИЖЕНИЯ

https://congress-vsp.ru/xv/