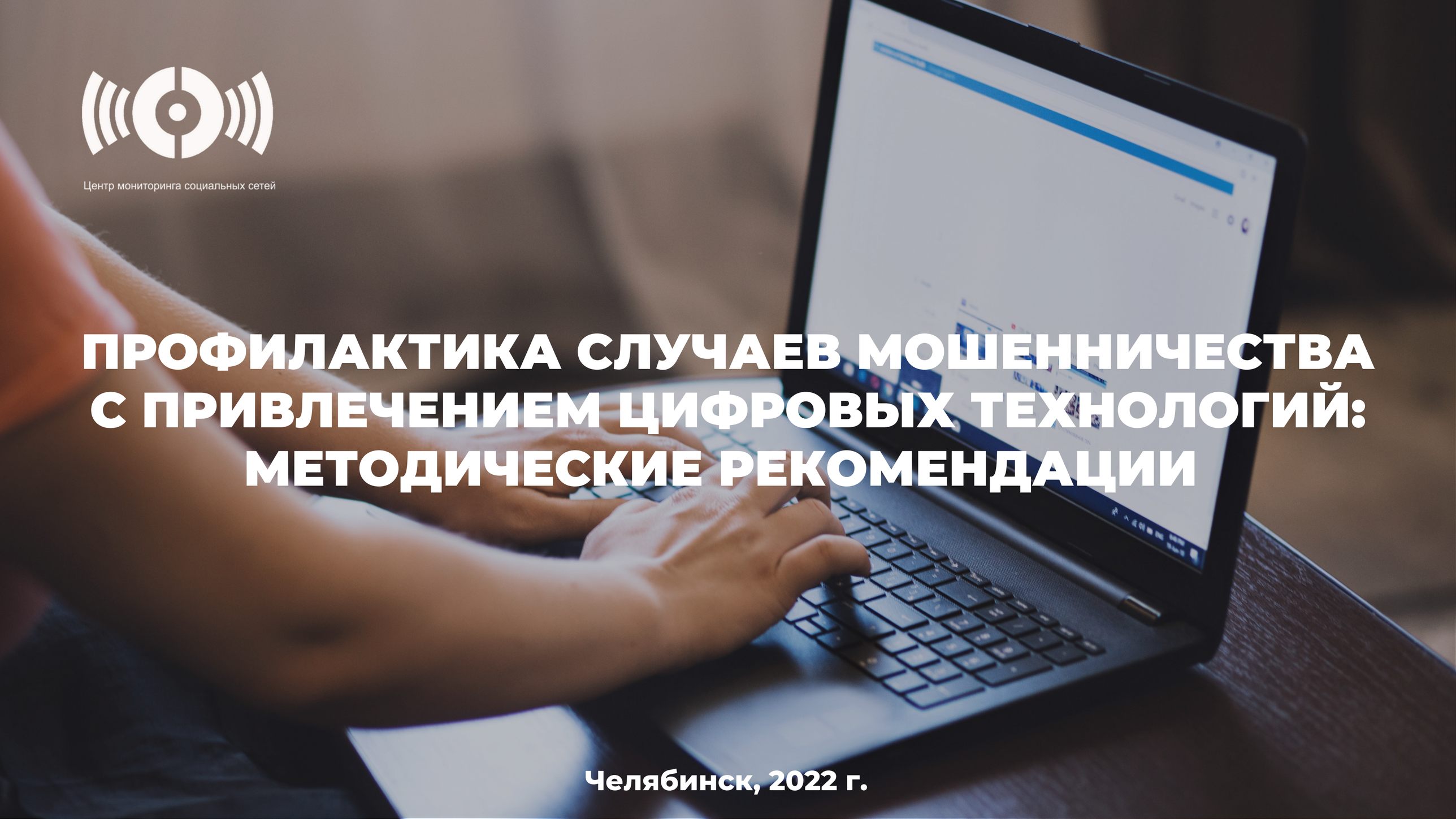


Центр мониторинга социальных сетей

ПРОФИЛАКТИКА СЛУЧАЕВ МОШЕННИЧЕСТВА С ПРИВЛЕЧЕНИЕМ ЦИФРОВЫХ ТЕХНОЛОГИЙ: МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

Челябинск, 2022 г.

СОДЕРЖАНИЕ

ЦЕНТР
МОНИТОРИНГА
СОЦИАЛЬНЫХ СЕТЕЙ
ГБУ ДПО ЧИРПО

ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО

ЦЕНТР
МОНИТОРИНГА
СОЦИАЛЬНЫХ СЕТЕЙ
ГБУ ДПО ЧИРПО

Мошенники используют следующие мотивы:

- **беспокойство за близких и знакомых;**
- **беспокойство за свой телефонный номер, счёт в банке или банковскую карту;**
- **желание выиграть крупный приз;**
- **любопытство – желание получить доступ к какой-либо информации;**
- **желание помочь больным детям или людям, пострадавшим от стихийных бедствий.**

Виды телефонного мошенничества:

1. Обман по телефону. С вас могут потребовать выкуп или взятку за освобождение якобы из отделения полиции или с места ДТП вашего родственника.
2. СМС-просьба о помощи.
3. Телефонный номер-грабитель. Платный номер, за звонок на который со счёта списывается денежная сумма.
4. Выигрыш в лотерее, которую якобы проводит радиостанция или оператор связи. Вас могут попросить оплатить пошлину, налог и т.п., перевести сумму на определённый счёт, сообщить пришедший на телефон код.
5. Штрафные санкции и угроза отключения номера якобы за нарушение договора с оператором вашей мобильной связи.
6. Ошибочный перевод средств. Вас попросят перевести якобы ошибочно переведённые средства, а затем дополнительно снимут деньги.

ФЕЙКОВЫЕ ЗВОНКИ, СМС

ЦЕНТР
МОНИТОРИНГА
СОЦИАЛЬНЫХ СЕТЕЙ
ГБУ ДПО ЧИРПО

Злоумышленники присылают на номер жертвы СМС с текстом о том, что ее карта заблокирована. В конце указывается номер телефона, по которому нужно связаться с якобы сотрудником банка. Звонок по указанному номеру может иметь несколько последствий: во-первых, это подключение платных услуг и списание денежных средств; во-вторых, это попадание на крючке к мошеннику-манипулятору и перевод для них денежных средств.

Важно:

1. Никогда и никому не сообщайте свои данные, а также любую банковскую информацию.
2. Сотрудники банка не будут звонить Вам первыми и просить сказать свои данные, единственная информация которая может потребоваться сотрудникам банка «кодовое слово» которое Вы оставляли в банке при подписании договора.
3. Если Вам поступает звонок от сотрудника полиции, то обязательно уточните Ф.И.О. сотрудника, должность, отделение полиции. Позвоните в отдел полиции по самому простому телефону – 02 и сообщите о сучившемся.
4. Информация от мошенника может быть связана с близким родственником. Важно не принимать информацию близко к сердцу, а стоит созвониться с родственником, о котором идет речь, и уточнить у него, где он находится в данный момент, все ли у него в порядке.

Как же избавиться от спам-звонков? Есть несколько вариантов:

- использовать встроенные возможности операционной системы вашего смартфона;

- воспользоваться предлагаемыми оператором услугами антиспама;

- установить специальное приложение для борьбы с телефонным спамом.

ВРЕДОНОСНЫЕ ССЫЛКИ

ЦЕНТР
МОНИТОРИНГА
СОЦИАЛЬНЫХ СЕТЕЙ
ГБУ ДПО ЧИРПО

Мошенники могут передавать сообщения с вредоносной информацией (ссылкой) через мессенджеры, при этом данная ссылка может приходить от неизвестного номера, рекламного агентства и т.д.:

Пример сообщений:

«здесь наши с тобой фото http:\\\\...»
«ваш аккаунт, страница «ВКонтакте» взломаны, пройдите регистрацию http:\\...»
«вы выиграли автомобиль, подробности http:\\...»

ЧТО НУЖНО ПОМНИТЬ?

1. При получении данного сообщения в мессенджере откажитесь от прохождения по указанной ссылке.
2. Не стоит скачивать присланные файлы от незнакомых пользователей, под прикрытием текстового документа в формате Word может содержаться вредоносная программа.
3. По всему миру активно распространяются вирусы-вымогатели, которые зашифровывают все файлы, находящиеся на пораженном устройстве, а "жертве" предлагается оплатить расшифровку собственных данных.

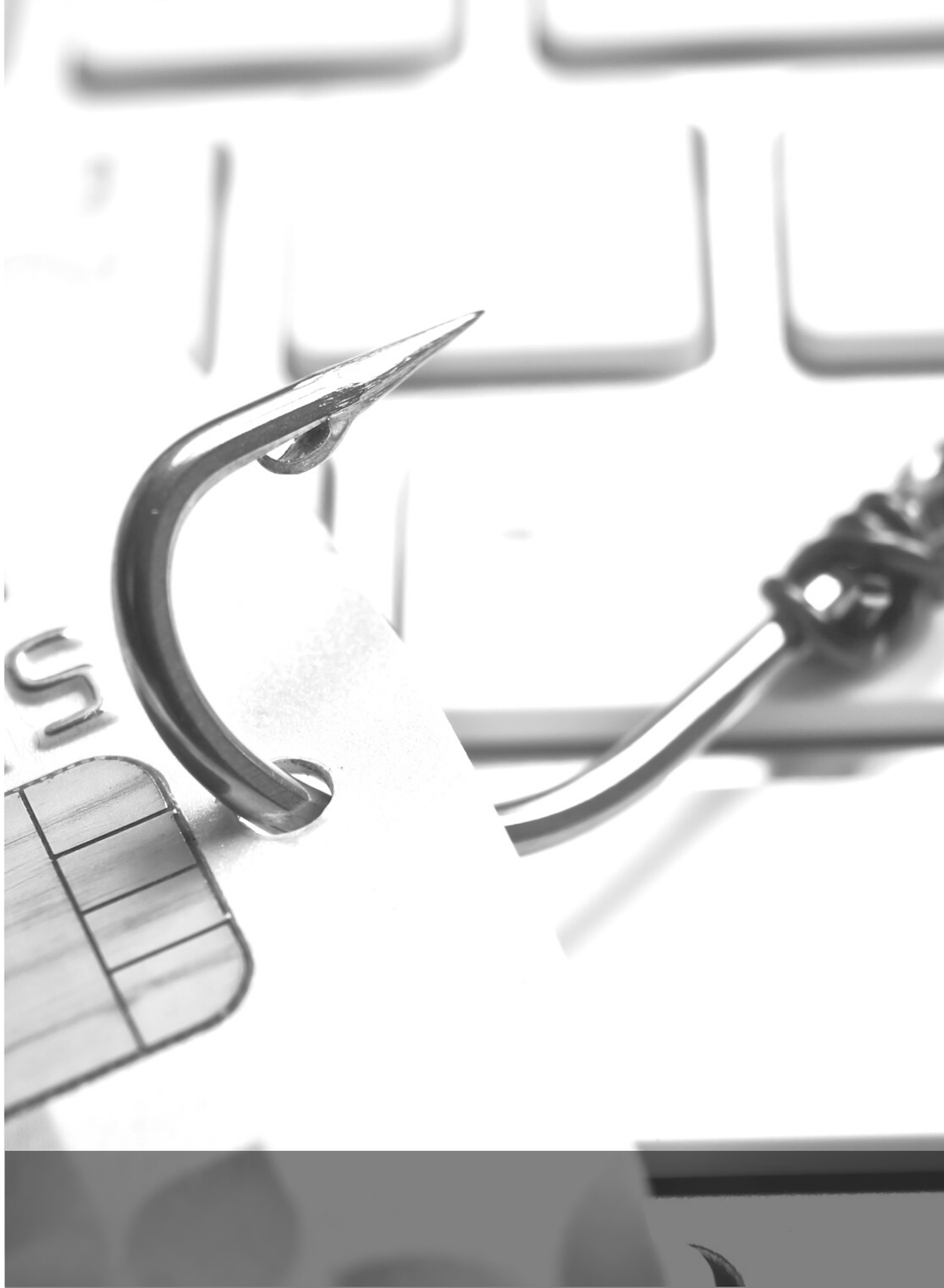
Цель мошенников: получение доступа к вашим счетам и вкладам. Технически вредоносная программа, попадая в ваше мобильное устройство или ПК, способна предоставлять злоумышленникам доступ к вашему устройству.

В случае заражения устройства рекомендуется срочно связаться с банком, заблокировать карту и приостановить обслуживание по счетам. На ПК рекомендуется запустить антивирусную программу.

МОШЕННИЧЕСТВО ПОСРЕДСТВОМ ФИШИНГОВЫХ САЙТОВ И САЙТОВ-ПОДДЕЛОК

Цель:

получить доступ к конфиденциальным данным пользователей — логинам и паролям. Это достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, образовательных организаций, а также личных сообщений внутри различных сервисов или социальных сетей. В письме часто содержится прямая ссылка или баннер, ведущий на сайт, внешне неотличимый от настоящего.



МОШЕННИЧЕСТВО ПОСРЕДСТВОМ ФИШИНГОВЫХ САЙТОВ И САЙТОВ-ПОДДЕЛОК

ЦЕНТР МОНИТОРИНГА СОЦИАЛЬНЫХ СЕТЕЙ ГБУ ДПО ЧИРПО

ВАЖНО:

Если при переходе на посещаемый вами сайт или сервис по ссылке, полученной в мессенджере или по электронной почте, браузер просит вновь ввести логин и пароль для входа — стоит обратить пристальное внимание на название сайта в адресной строке.

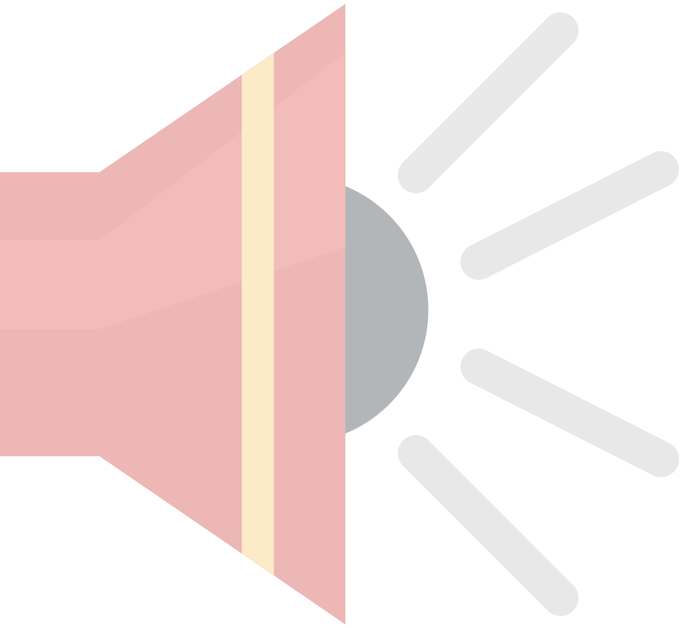
Для того, чтобы обезопасить доступ к персональному аккаунту в социальных сетях, настоятельно рекомендуется установить двухфакторную аутентификацию - таким образом при входе в аккаунт с нового устройства вам на телефон будет приходить смс с кодом подтверждения.

При совершении покупок в онлайн-магазинах, особенно не проверенных брендов и сервисов (дешевые авиабилеты, необычные сайты одежды), не регистрируйтесь посредством своего аккаунта в социальных сетях (быстрая регистрация) —- лучше создать новую учетную запись.

При оплате банковской картой в онлайн магазине, старайтесь совершать это в безопасном режиме. Чаще всего браузер предложит им воспользоваться автоматически, если нет, это может служить поводом насторожится.

ОСНОВНЫЕ СОВЕТЫ ПО БОРЬБЕ С ФИШИНГОМ (ИНТЕРНЕТ-МОШЕННИЧЕСТВО):

ЦЕНТР МОНИТОРИНГА СОЦИАЛЬНЫХ СЕТЕЙ ГБУ ДПО ЧИРПО



- Следите за своим аккаунтом. Если ты подозреваешь, что Ваша анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее;
- Используйте безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем;
- Используйте сложные и разные пароли. Таким образом, если Вас взломают, то злоумышленники получат доступ только к одному Вашему профилю в сети, а не ко всем;
- Если Вас взломали, то необходимо предупредить всех своих знакомых, которые добавлены у Вас в друзьях, о том, что Вас взломали и, возможно, от Вашего имени будет рассылаться спам и ссылки на фишинговые сайты;
- Установите надежный пароль (PIN) на мобильный телефон;
- Отключите сохранение пароля в браузере.

РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ БАНКОВСКИХ ПРИЛОЖЕНИЙ:

ЦЕНТР МОНИТОРИНГА СОЦИАЛЬНЫХ СЕТЕЙ ГБУ ДПО ЧИРПО

- Не указывать номера мобильных устройств, используемых для работы с банковскими картами и дистанционного управления банковским счетом, как контактных в сети Интернет, в объявлениях и на страницах социальных сетей (одна sim-карта для общения, вторая для сервисов, связанных с банками и государственными услугами);

- При заключении договора с банком уточнить возможность указать в договоре, либо в иной форме согласовать с банком, что управление банковским счетом и проведение операций по карте может осуществляться только с одного мобильного устройства с одним IMEI, ограничить круг операций, установить лимит денежных средств, который можно переводить с помощью мобильного устройства;

- Запретить перевод всего объема денежных средств с карты, счета – установите лимит.

РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ БАНКОВСКИХ ПРИЛОЖЕНИЙ:

ЦЕНТР
МОНИТОРИНГА
СОЦИАЛЬНЫХ СЕТЕЙ
ГБУ ДПО ЧИРПО

В современных условиях встречается достаточно часто, предполагает ваш добровольный перевод денежных средств на благотворительность (например сбор денежных средств на лечение детей или животных), срочная просьба о помощи близкого или знакомого человека с его страницы.

Что делать, если вас взломали на примере VK:

Выполните полную проверку антивирусом.
Смените пароль на новый на странице ВК («Настройки» → «Изменить пароль»), на привязанном к ней ящике электронной почты и других важных сайтах.
Если доступ к странице не удаётся восстановить с помощью ссылки «Забыли пароль?», обратитесь в службу поддержки со страницы другого пользователя за помощью.

Важно:

1. Если вы хотите участвовать в благотворительности, это лучше всего делать через проверенные фонды или организации. В социальных сетях чаще всего собирают денежные средства мошенники.
2. Если сообщение в социальной сети о просьбе помочь Вас действительно затронуло обратите внимание на следующие обстоятельства перед переводом денежных средств: соответствует ли фамилия и город проживания с указанными реквизитами блага получателя, если упоминания о предыдущем опыте сбора средств сети, через поисковые системы проверти фотографии на предмет их подлинности.
3. В случае финансовой просьбе о помощи Вашего близкого обратите внимание: указана ли цель просьбы, может ли человек назвать какие-то факты известные только вам, не поленитесь позвонить и лично уточнить ситуацию.

ФЕЙКОВЫЕ БИЛЕТЫ В ТЕАТР И КИНО

ЦЕНТР
МОНИТОРИНГА
СОЦИАЛЬНЫХ СЕТЕЙ
ГБУ ДПО ЧИРПО

Покупать билеты в культурные заведения - театр, музей или на концерт намного удобнее онлайн. Однако, порой поиски нужного сайта могут привести как на официальную страницу организации, так и на ресурс перекупщиков и мошенников. Данные сайты похожи внешне и имеют подобное содержание.

Важно:

1. **Не кликайте на самые первые сообщения в поисковой выдаче, скорее всего это будут рекламные сообщения.**
2. **Вот признаки, которые выдают мошенников:**

- Сайт создали недавно – всего пару дней назад.
- У театра много адресов – и все ненастоящие.
- Не получается связаться с администрацией театра.
- Купить билет предлагают только на сайте.
- Сайт не дает выбрать место в зале.

Чем настоящий театр отличается от фальшивого

Настоящий театр	Фальшивый театр
Продает билеты на сайте и в кассе	Продает билеты только на сайте
Предлагает выбрать ряд и место в зале	Предлагает выбрать ряд
Указывает рабочие телефоны и электронную почту сотрудников, ссылки на соцсети	Указывает контакты, по которым невозможно дозвониться или написать
Работает в одном городе, иногда объявляет о гастролях в других городах	Работает чуть ли не во всех городах Росси

КИБЕРМОШЕННИЧЕСТВО В ФОРМАТЕ ОПРОСОВ, КОНКУРСОВ И ВИКТОРИН

ЦЕНТР
МОНИТОРИНГА
СОЦИАЛЬНЫХ СЕТЕЙ
ГБУ ДПО ЧИРПО

Распространенным видом Интернет-мошенничества является мошенничество с использованием электронной почты, в которой жертвам сообщают, что они выиграли в лотерею. Такие мошенники сообщают получателям, что они смогут получить свой приз только после уплаты небольшой суммы.
Мошенники с лотерейными взносами обычно составляют электронные письма так, чтобы они выглядели и звучали правдоподобно. Афера направлена на мечты людей выиграть огромные суммы денег, даже если они, возможно, никогда не покупали лотерейных билетов.

Важно: ни одна законная лотерейная схема не будет просить победителей заплатить, чтобы получить свой приз.

Важно:

1. В процессе общения в социальных сетях злоумышленник постепенно переходит к более личным вопросам, поэтому будьте осторожны с онлайн-знакомствами и не раскрывайте своих персональных данных, личной информации в сомнительных опросах в сети.
2. Помните, что нельзя выиграть в лотерею, получить налоговый вычет и субсидию от государства, предварительно не купив лотерейный билет и подготовив пакет документов.
3. Помните, чтобы органы государственной власти и ведомства не высылают документы о Ваших задолженностях и штрафах на вашу личную электронную почту данная информация может быть размещена на портале государственных услуг.

ЦЕНТР
МОНИТОРИНГА
СОЦИАЛЬНЫХ СЕТЕЙ
ГБУ ДПО ЧИРПО

КРАТКИЕ РЕКОМЕНДАЦИИ ПО СНИЖЕНИЮ УРОВНЯ УЯЗВИМОСТИ ПЕРЕД УГРОЗАМИ СО СТОРОНЫ IT-ПРЕСТУПЛЕНИЙ

КАК РЕАГИРОВАТЬ НА МОШЕННИКОВ И ВЫМОГАТЕЛЕЙ

ЦЕНТР
МОНИТОРИНГА
СОЦИАЛЬНЫХ СЕТЕЙ
ГБУ ДПО ЧИРПО

- **Старайтесь сохранять спокойствие, состояние паники - это то, что хотят вызвать у вас злоумышленники.В таком состоянии человек не способен использовать критическое мышление.**
- **В РФ органы государственный власти, ведомства и службы не высылают документы гражданам на личную почту. Штрафы, повестки и прочие документы проходят на портале Государственных услуг.**
- **Передача персональных данных и личной информации третьим лицам недопустима. Мошенники часто говорят о подозрительных операциях, или иной активности как с вашими счетами и вкладами, так и с их получением. Сотрудники банка могут уточнить у вас для идентификации только кодовое слово оставленное вами при регистрации.**
- **Нельзя выиграть в лотерею или получить налоговый вычет случайно, предварительно не предпринимая никаких действий.**
- **Электронные письма, которые приходят к Вам, могут содержать вредоносные ссылки или программы, а следовательно, не стоит переходить по незнакомым ссылкам, сохранять подозрительные файлы. А также верить провокации, что ваши данные были украдены и вам нужно перевести денег для их спасения.**
- **Любую информацию, касающуюся ваших действий, стоит перепроверять. Мошенники могут представится банком, полицией, органом власти. Помните, что сегодня существует возможность подмены номера.**

ВАЖНО ОБРАЩАТЬ ВНИМАНИЕ ЕСЛИ ВАМ ПРЕДЛАГАЮТ:

ЦЕНТР МОНИТОРИНГА СОЦИАЛЬНЫХ СЕТЕЙ ГБУ ДПО ЧИРПО

- назвать номер банковской карты, трёхзначный код на оборотной стороне карты, ПИН-код;
- произвести манипуляции с банковской картой у банкомата;
- сообщить пришедший на телефон код;
- перевести сумму денег (аванс, залог, пошлина, налог, ошибочно переведённый платеж и т.п);
- перейти по ссылке в Интернете, в СМС- или ММС-сообщении на смартфоне;
- позвонить по указанному в СМС-сообщении номеру телефона;
- отправить ваш номер телефона;
- отправить СМС-сообщение на короткий номер;
- назвать пароли от ваших личных страничек в социальных сетях.

ИТОГО.
КЛЮЧЕВЫЕ РЕКОМЕНДАЦИИ

ЦЕНТР
МОНИТОРИНГА
СОЦИАЛЬНЫХ СЕТЕЙ
ГБУ ДПО ЧИРПО

1. Создайте уникальный и надежный пароль для каждого сайта.
2. Не переходите по ссылкам в письмах или сообщениях от неизвестных отправителей.
3. Проверяйте детали: опечатки в адресе сайта, странные доменные зоны и ошибки в текстах — признаки опасных страниц.
4. Не публикуйте личные данные на подозрительных сайтах, такие как номер телефона, адрес электронной почты, номер кредитной карты.
5. Не стоит доверять сообщениям о подарках и внезапных выигрышах, особенно если Вы не участвовали в розыгрышах.
6. Используйте актуальные версии браузеров, антивирусных программ.
7. Периодически проверяйте свой гаджет на наличие вирусов и вредоносных программ. При обнаружении, их необходимо вылечить и обезвредить.
8. При потере своей банковской карты, необходимо обратиться в банк и заблокировать карту. Не забывайте периодически следить за вашей банковской активностью. В случае странных действий, которые Вы не совершали, обратитесь в банк.
9. Приобретайте услуги и вещи только на проверенных сайтах.
10. Используйте антивирусные программы и устанавливайте СМС верификацию входа в аккаунт.

Контактная информация

Центр мониторинга социальных сетей ГБОУ ДПО ЧИРПО

+7 (351) 222 07 56 (доп. 126)
kiber-lab@ya.ru

Центр мониторинга социальных сетей ГБУ ДПО ЧИРПО

https://chirpo.ru/monitoring-social

Онлайн-консультант по вопросам медиабезопасности

www.resurs-centr.ru

Горячая линия «Экстремизму - НЕТ!»

https://resurs-center.ru/hotline

Виртуальная горячая линия по проблемам кибербезопасности

https://resurs-center.ru/

Если Вы стали жертвой преступления в обязательном порядке необходимо обращаться в полицию по телефону 112 или 02!