ЦИФРОВЫЕ ВОЛОНТЕРЫ

МЕТОДИЧЕСКОЕ ПОСОБИЕ
ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ УЧАСТНИКОВ ПРОЕКТА «ЦИФРОВОЙ РОСТ 2.0»

Автономная некоммерческая организация по содействию развития цифровых компетенций молодёжи и профилактике негативных явлений в информационной среде «Цифровые волонтеры»

Москва, 2024

УДК 004.056.5
ББК 16.8

Методическое пособие по информационной безопасности для участников проекта «Цифровой рост 2.0» / Под ред. С. В. Большакова, Е. М. Пащенко, Г. В. Пащенко. М.: АНО «Цифровые волонтеры», 2024. 20 с.

В методическое пособие по информационной безопасности включены материалы, которые содержат основные правила, методы противодействия злоумышленникам в сети Интернет, составлены алгоритмы действий, согласно которым подросток сможет четко понимать, как ему поступить в ситуациях, создающих угрозу безопасности его персональных данных.

Проект «Цифровой рост 2.0» реализуется в рамках конкурса грантов «Москва-добрый город» при поддержке Департамента труда и социальной защиты населения города Москвы

Содержание

Введение

В современном мире цифровые технологии стали неотъемлемой частью повседневной жизни. С каждым годом растёт доступ к интернету и мобильным устройствам, что открывает новые возможности для общения, обучения, работы и ведения бизнеса.

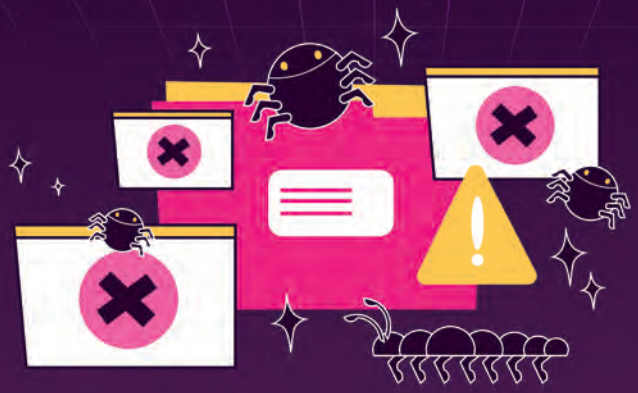
Однако с распространением технологий также увеличивается угроза киберпреступлений, которые могут наносить серьёзный ущерб как отдельным пользователям, так и обществу в целом.

Цифровая грамотность стала критически важной для успешного противодействия киберугрозам. Это знание и понимание того, как безопасно использовать технологии, идентифицировать потенциальные угрозы и защищать личные данные.

Без достаточного уровня цифровой грамотности пользователи становятся легкой мишенью для мошенников, что может привести к утечкам информации, финансовым потерям и даже к правовым последствиям.

Введение понятия цифровой грамотности в образовательные программы и увеличение осведомлённости о киберугрозах представляют собой ключевые шаги в создании защищённой цифровой среды. Понимание рисков и методов защиты может значительно снизить вероятность того, что люди станут жертвами киберпреступников.

Цифровая грамотность играет ключевую роль в борьбе с киберпреступностью, позволяя пользователям не только защищать себя, но и формировать более безопасное цифровое общество. Повышение уровня цифровой грамотности является необходимостью в условиях быстро меняющегося мира технологий и усиления киберугроз. Инвестиции в образование и просвещение в области кибербезопасности должны стать приоритетом для каждого из нас.



Современные киберугрозы в 2024 году

1 **Вербовка через шантаж.**

Использование информации о человеке для принуждения его к выполнению определённых действий, включая денежные выплаты или участие в незаконной деятельности.

2 **Пассивное участие в трафике «чёрных денег».**

Пользователи ненамеренно становятся частью схем по отмыванию денег, когда их устройства используются для обработки или передачи незаконных денег без их ведома.

3 **Закладчики взрыв пакетов.**

Угрозы, связанные с использованием дистанционно управляемых устройств или программ, предназначенных для нанесения физического ущерба путём взрыва.

4 **Мошеннический VPN.**

Использование поддельных или небезопасных VPN-сервисов, которые могут отслеживать личные данные пользователей, собирать информацию или предлагать пользователю спам и вредоносные программы.

5 **Обход заблокированных ресурсов.**

Методы обхода ограничений на доступ к контенту, которые могут подвергать пользователей риску кибератак и потерей персональной информации.

Эти угрозы требуют тщательной осторожности и принятия мер предосторожности, таких как использование надёжного ПО, осведомленность о безопасности и соблюдение законов.

Вербовка через шантаж

Вербовка через шантаж — манипуляция, при которой злоумышленник использует личную информацию о жертве для принуждения его к выполнению требований, например, вымогание денег, предоставление услуг или участие в незаконной деятельности.

Механизм

1 **Сбор информации:**

Злоумышленники могут собирать информацию через социальные сети, взлом аккаунтов, перехват данных или с помощью различных методов социальной инженерии. Их интересует личная информация - фотографии, сообщения или денежные операции.

2 **Угрозы:**

Получив информацию, злоумышленник угрожает раскрыть её (например, опубликовать в интернете, отправить родителям), если жертва не выполнит его требования. Угрозы могут быть как прямыми, так и скрытыми, создавая атмосферу страха.

3 **Действия жертвы:**

Жертва, находясь под давлением, может согласиться выполнять требования. Это могут быть вымогательства, денежные компенсации, участие в преступной деятельности, действия против своих моральных принципов.

4 **Цикл вербовки:**

Злоумышленники могут повторно манипулировать жертвой.

Примеры вербовки

Компрометирующие фотографии:

Злоумышленник получает доступ к личной информации или фотографиям жертвы (например, через взлом аккаунта в соцсетях). Угрожает публичным распространением этих материалов, если жертва не выполнит его требования, такие как отправка денег или участие в преступной деятельности.

Давление в учебном заведении:

Угроза публичного позора, если тот не выполнит определённые задачи (например, доставить подозрительный предмет по указанному адресу). Шантаж может также происходить на основе личных слабостей (например, использование конфиденциальной информации о здоровье).

Соблазн через знакомства:

Злоумышленник может завести романтические отношения с целью получения личной информации, а затем угрожать раскрытием этой информации, если жертва не выполнит его требования.

Защита

Безопасность данных:

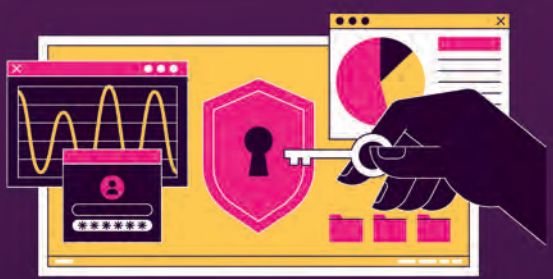
Использование двухфакторной аутентификации, регулярные изменения паролей и шифрование информации.

Осведомлённость о угрозах:

Осведомлённость о возможных мошеннических схемах и признаках шантажа помогает распознать угрозу на ранней стадии.

Психологическая поддержка:

Важно иметь доступ к ресурсам поддержки, таким как психологи или группы поддержки, чтобы справиться с последствиями шантажа.



Вербовка через шантаж остается актуальной угрозой в современном цифровом мире, требующей высокой степени осведомленности и готовности к защите личной информации.

Пассивное участие в трафике «чёрных денег»

Пассивное участие в трафике «чёрных денег» подразумевает участие жертвы в незаконном переводе денег или схемах отмывания денег, где их устройства, аккаунты или интернет-соединения могут скрыто использоваться.

Как это происходит?

1 **Использование заражённых устройств.**

Злоумышленники могут заразить устройства (компьютеры, смартфоны) вредоносным ПО, которое будет выполнять следующие функции:

- Перехват данных об учётных записях и банковских картах.
- Установка скрытых программ для создания «ботнетов», которые обеспечивают анонимный трафик в целях отмывания денег.

2 **Злоупотребление учётными записями.**

Хакеры могут получить доступ к учётным записям (например, в банках или платёжных системах) и использовать их для переводов «черных» денег между разными счетами, что затрудняет их отслеживание.

3 **Переадресация трафика.**

Незаконные организации могут использовать сеть жертв для перенаправления трафика, создавая видимость законных операций. Жертвы могут даже не подозревать, что их Интернет-соединение используют для отмывания денег, например, через прокси-сервер.

4 **Обман через анонимные криптовалюты.**

В связи с ростом популярных анонимных криптовалют (например, Monero, Dash), злоумышленники используют их для скрытия источника денег. Жертвы могут стать непреднамеренными участниками этих операций, если их устройства используются для перевода криптовалюты.

Риски

Правовые последствия:

Если правоохранительные органы обнаружат участие жертвы в этих схемах, это может привести к уголовной ответственности, даже если они не были осведомлены о своих действиях.

Денежные потери:

Заражённые устройства могут привести к краже денег с банковских счётов жертвы.

Утечка личной информации:

Вредоносное ПО может также собирать и передавать личную информацию, что приводит к дополнительным угрозам, таким как утечка данных, кража игровых аккаунтов и т.п.

Защита

1 **Антивирусные и антишпионские программы.**

Установка и регулярное обновление программ для защиты от вирусов и шпионского ПО помогает предотвратить заражение.

2 **Бдительность при использовании интернета.**

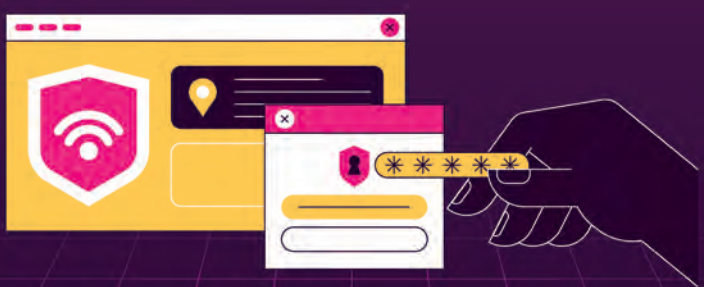
Избегать переходов по подозрительным ссылкам, открывать письма только от проверенных отправителей и не скачивать файлы из ненадёжных источников.

3 **Мониторинг финансовых операций.**

Регулярная проверка своих банковских счетов и операций на предмет подозрительной активности может помочь выявить проблемы на ранних стадиях.

4 **Обучение и информированность.**

Знание о методах мошенничества и отмывания денег поможет пользователям лучше защищать свои устройства и личные данные.



Закладчики взрыв пакетов

Закладчики взрывных устройств является новым вызовом в современной истории нашей страны. Злоумышленники используют подростковую молодежь посредством онлайн-вербовки, для закладки устройств или программ, предназначенные для запуска атак, которые могут повредить здания, нанести вред человеку или создать хаос в определённых обстоятельствах.

Онлайн-вербовка - это процесс привлечения и манипуляции людьми через интернет для участия в создании, распространении или активации взрывных устройств. Эти действия могут быть частью организованной преступной или террористической деятельности и наносят значительный ущерб как отдельным лицам, так и обществу в целом.

Механизм работы

1 **Подготовка взрывного устройства.**

Создание взрывного устройства может включать использование доступных материалов, но в киберпреступности часто речь идёт о дистанционно управляемых устройствах (например, самодельные взрывные устройства, управляемые через интернет).

2 **Инфраструктура для запуска.**

Злоумышленники используют уязвимости в различных системах или в оборудовании для запуска атаки, например, доступ к системам управления (промышленные контроллеры, системы HVAC и т.д.), вхождение в сети, где есть системы безопасности, которые можно обойти.

3 **Использование программного обеспечения.**

Закладчики могут представлять собой вредоносные программы или скрипты, которые устанавливаются на компьютер или сервер. Они могут активировать компоненты атакующего устройства, отправляя команды или запускаются автоматически при выполнении определённых условий.

4 **Активация взрывного устройства.**

После того как закладчик получает команду или достигает определённых условий, он активирует взрывное устройство, что может привести к разрушительным последствиям, такими как: взрыв, который может повредить объекты или повредить людей, использование в террористических актах или актах мести.

Последствия

1 **Участие в криминальной деятельности.**

Лица, ставшие жертвами вербовки, могут быть вовлечены в преступные действия, которые могут привести к уголовной ответственности.

2 **Грозящие угрозы обществу.**

Закладка взрывных устройств несет опасность для жизни и здоровья граждан, а также создает атмосферу страха и нестабильности в обществе.

3 **Психологическое воздействие.**

Подобные действия ведут к психоэмоциональному стрессу как для исполнителей, так и для жертв потенциальных атак.

4 **Уничтожение инфраструктуры.**

Взрывы могут разрушать здания, нарушать общественный порядок и приводить к финансовым убыткам для бизнеса и государства.

Методы вербовки

1 **Социальные сети и мессенджеры.**

Злоумышленники используют платформы, такие как Telegram, WhatsApp, социальные сети, для поиска и общения с потенциальными жертвами или исполнителями. Используются закрытые группы или каналы для обмена информацией и приглашений.

2 **Форумы и специализированные сайты.**

Создание и использование анонимных форумов, где собираются сторонники радикальных идеологий или криминальной активности. Участники обсуждают методы, технологии и подходы к вербовке новых участников.

3 **Манипуляция уязвимыми группами.**

Вербовка людей, которые могут быть в уязвимом положении (например, подростков или молодежи), с использованием обещаний о "друзьях", "профессии" или финансовых вознаграждениях.

4 **Психологическое давление и запугивание.**

Использование угроз или шантажа для принуждения людей к выполнению задач, включая закладку взрывных устройств.

5 **Использование технологий.**

Инструкции по созданию взрывных устройств или закладок могут распространяться через видеоуроки, электронные книги или инструкции, размещенные на анонимных платформах.

Мошеннический VPN

Мошеннический VPN — это виртуальная частная сеть, предлагающая услуги по обходу географических ограничений и шифрованию интернет-трафика, но фактически не обеспечивающая обещанной безопасности и конфиденциальности.

Вместо этого они могут отслеживать пользовательские данные, продавать их третьим лицам или устанавливать вредоносные программы на устройства пользователя.

Признаки мошеннического VPN

1 **Отсутствие прозрачности.**

Неясная политика конфиденциальности, отсутствие информации о владельцах сервиса или местоположении серверов.

2 **Практически бесплатный.**

Очень дешёвые или бесплатные VPN могут быть заманчивыми, но часто имеют скрытые сборы или недоступные функции.

3 **Низкая скорость и стабильность соединения.**

Неэффективные и перегруженные серверы могут приводить к постоянным сбоям и низкому качеству соединения.

4 **Реклама и спам.**

Частые всплывающие окна с рекламой или предложения загрузить дополнительные приложения.

5 **Сбор данных.**

Некоторые VPN могут сохранять журналы активности или собирать личные данные, такие как адреса электронной почты и данные банковских карт.

Риски использования мошеннического VPN

Утечка личной информации.

VPN могут отслеживать пользовательскую активность, сохраняя данные, которые могут быть использованы для мошенничества.

Заражение вредоносным ПО.

Некоторые приложения могут содержать шпионские или вирусные программы, что ставит под угрозу безопасность устройства.

ЦИФРОВЫЕ ВОЛОНТЕРЫ

digital-volunteers.ru

info@digital-volunteers.ru

115191, г. Москва, пер. Холодильный, 3к1 стр. 2

Автономная некоммерческая организация
по содействию развития цифровых компетенций
молодёжи и профилактике негативных явлений
в информационной среде «Цифровые волонтеры»

Методическое пособие разработано и подготовлено
для проекта «Цифровой рост 2.0» и распространяется
бесплатно.

при поддержке:

Москва – добрый город

ДЕПАРТАМЕНТ ТРУДА И СОЦИАЛЬНОЙ ЗАЩИТЫ НАСЕЛЕНИЯ ГОРОДА МОСКВЫ