**Социальная инженерия и способы защиты от мошеннических действий**

Социальная инженерия — это совокупность психологических и социологических приёмов, методов и технологий, которые позволяют получить доступ к конфиденциальной информации.

Следует отметить, что по итогам 1 полугодия 2024 года в Воронежской области отмечено увеличение на 18,8 % числа зарегистрированных мошенничеств (с 2 223 до 2 642), а также на 10,1 % преступлений, связанных с использованием сети «Интернет» (с 2 300 до 2 634), что свидетельствует об актуальности данного направления профилактики.

Человеческий фактор по-прежнему остается слабым звеном в любой системе защиты, поэтому сегодня как никогда возрастает потребность в обучении граждан основам информационной безопасности.

**Методы социальной инженерии**

***Фишинг***

Метод сбора пользовательских данных для авторизации — обычно это массовые рассылки спама по электронной почте. В классическом сценарии на почту жертвы приходит поддельное письмо от какой-то известной организации с просьбой перейти по ссылке и авторизоваться (ввод комбинации логин/пароль). Чтобы вызвать больше доверия, мошенники придумывают серьёзные причины для перехода по ссылке: например, просят потенциальную жертву обновить пароль или ввести различного рода персональную информацию (ФИО, номер телефона, должность и т.д.).

***Троян***

Вирус не зря получил своё название по принципу работы троянского коня из древнегреческого мифа. Только приманкой здесь становится email-сообщение, которое при классическом сценарии мошенников обещает быструю прибыль, выигрыш или другие «золотые горы» — но в результате человек получает вирус, с помощью которого злоумышленники крадут его данные.

Часто граждане непреднамеренно помогают злоумышленнику в развитии атаки, пересылая зараженное письмо коллегам с просьбой открыть вложение или перейти по ссылке.

***Дорожное яблоко***

Представляет собой адаптацию троянского коня и состоит в использовании физических носителей (CD, флэш-накопителей). Злоумышленник обычно подбрасывает такой носитель в общедоступных местах.

***Услуга за услугу***

Используя этот метод, злоумышленник представляется сотрудником службы технической поддержки и спрашивает о наличии сбоев в работе программного обеспечения, предлагает исправить возникшие неполадки в системе либо предупредить о вероятности их наступления, хотя на самом деле проблем в работе ПО не возникало.

Распространенный сценарий, когда пользователь сам говорит об отсутствии времени и сообщает необходимые пароли для того, чтобы сотрудник технической поддержки самостоятельно провел необходимые манипуляции.

***Обратная социальная инженерия***

На электронную почту поступает письмо, информирующее о возможных сбоях в работе часто используемого программного обеспечения. В этом же письме указаны контактные данные специалиста технической поддержки, используемые злоумышленником. При возникновении сбоя в работе вышеперечисленного ПО, пользователь вспоминает о ранее поступившем предупреждении и связывается со злоумышленником в лице технического специалиста.

Таким образом, ситуация заранее подстроена, пользователь связывается с социальным хакером. Налаживая работу ПО, производятся необходимые для взлома манипуляции.

**Основные меры по защите от вышеперечисленных видов социальных атак**

1. **Сохраняйте бдительность**. Всегда обращайте внимание на отправителя писем и адрес сайта, где собираетесь ввести какие-то личные данные. Если это почта на домене крупной организации, удостоверьтесь, что домен именно такой и в нём нет опечаток. Если есть сомнения — свяжитесь с техподдержкой или представителем организации по официальным каналам.
2. **Используйте только проверенные носители информации**.
3. **Не переходите на подозрительные сайты и не скачивайте сомнительные файлы**.
4. **Не используйте один и тот же пароль** для доступа к личным и рабочим ресурсам.
5. **Использование антивирусного программного обеспечения**.

Ссылки на социальные видеоролики по теме статьи:

https://disk.yandex.ru/i/WaxOnz8zzDpXQQ

https://disk.yandex.ru/i/VgQM6cWLVCat8g

https://disk.yandex.ru/i/I06gdo2qjz7PAQ

https://disk.yandex.ru/i/VieGq2HBFI9bcg