СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

Информационый материал в рамках реализации Стратегии повышения финансовой грамотности в РФ

Социальная инженерия (social engineering)

или «атака на человека» — это **совокупность психологических и социологических приёмов, методов и технологий, которые позволяют получить конфиденциальную информацию.**

В настоящее время социальная инженерия приобрела прочную связь с киберпреступностью, но на самом деле это понятие появилось давно и изначально не имело выраженного негативного оттенка.

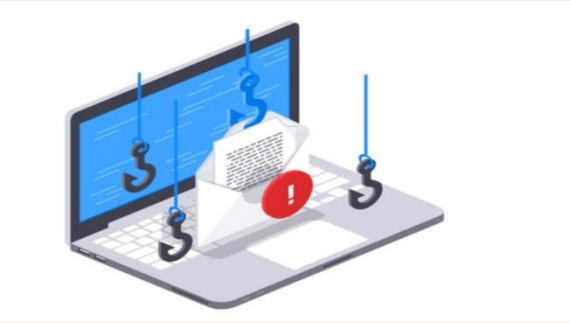
Люди использовали социальную инженерию с древних времён. Например, в Древнем Риме и Древней Греции очень уважали специально подготовленных ораторов, способных убедить собеседника в его «неправоте». Эти люди участвовали в дипломатических переговорах и работали на благо своего государства.

Методы социальной инженерии

«Фишинг» (рыбная ловля)

– это получение личных данных пользователей для авторизации.

В классическом сценарии на электронную почту жертвы приходит поддельное письмо от какой-либо известной организации с просьбой перейти по ссылке и авторизоваться. Чтобы вызвать больше доверия, мошенники придумывают серьёзные причины для перехода по ссылке: например, просят жертву обновить пароль или ввести какую-то информацию (ФИО, номер телефона, банковской карты и даже CVV-код!). При нажатии по имеющейся ссылке происходит переадресация на сайт с формой, где человек вводит свои данные, которые становятся доступны мошеннику.



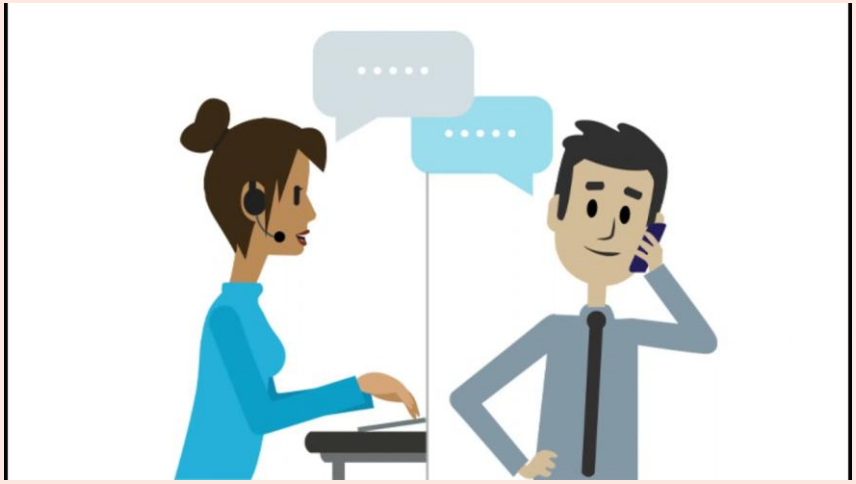
«Претекстинг»- это действие, отработанное по заранее составленному сценарию (претексту).

В результате цель (жертва) должна выдать определённую информацию, или совершить определённое действие.

Этот вид атак применяется обычно по телефону.

Обманщик звонит будущей жертве и просит выполнить ряд действий, на которые тот не пошел бы в ином случае. Например, перевести средства на «безопасный счет» или отправить по почте конфиденциальный служебный материал.

Вымогатель должен обладать начальными данными о том, кого собирается обмануть: имя, фамилия и отчество, город проживания, возраст, место работы.



«Троянский конь»

- *Эта техника эксплуатирует любопытство, либо алчность цели. Злоумышленник отправляет e-mail, содержащий во вложении важное обновление антивируса, или даже свежий компромат на сотрудника. Такая техника остаётся эффективной, пока пользователи будут слепо кликать по любым вложениям.*

«Дорожное яблоко»

- *Этот метод атаки представляет собой адаптацию троянского коня, и состоит в использовании физических носителей. Злоумышленник может подбросить инфицированный CD, или карту памяти, в месте, где носитель может быть легко найден (коридор, лифт, парковка). Носитель подделывается под официальный, и сопровождается подписью, призванной вызвать любопытство.*

- *Пример: Злоумышленник может подбросить CD, снабжённый корпоративным логотипом, и ссылкой на официальный сайт компании цели, и снабдить его надписью «Заработная плата руководящего состава ». Диск может быть оставлен на полу лифта, или в вестибюле. Сотрудник по незнанию может подобрать диск, и вставить его в компьютер, чтобы удовлетворить своё любопытство.*

«Квид про кво» **(от лат. *Quid pro quo* — «то за это») — услуга за услугу.**

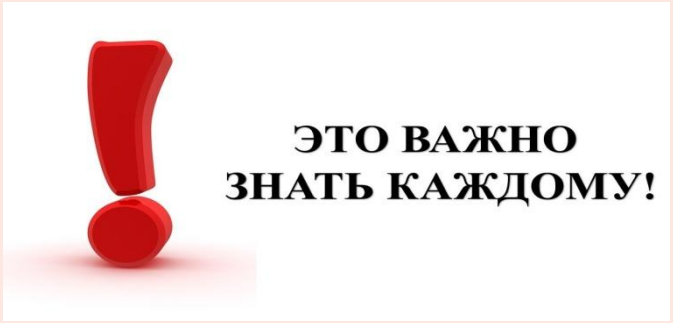
- *Злоумышленник может позвонить по случайному номеру в компанию, и представиться сотрудником техподдержки, опрашивающим, есть ли какие-либо технические проблемы. В случае, если они есть, в процессе их «решения» цель вводит команды, которые позволяют злоумышленнику запустить вредоносное программное обеспечение.*

«Обратная социальная инженерия»

Целью обратной социальной инженерии является заставить цель саму обратиться к злоумышленнику за «помощью». С этой целью злоумышленник может применить следующие техники:
Диверсия: Создание обратимой неполадки на компьютере жертвы.
Реклама: Злоумышленник подсовывает жертве объявление вида «Если возникли неполадки с компьютером, позвоните по такому-то номеру» (это в большей степени касается сотрудников, которые находятся в командировке или отпуске).

СПОСОБЫ ЗАЩИТЫ

- На постоянной основе **обновлять защиту от вирусов и вредоносного программного обеспечения.** В ней реализуются новые компоненты защиты, которые позволят избежать фишинговых ссылок и писем. Установка антивируса – отличный способ разобраться с подобной проблемой.
- Регулярно **обновляйте все свое программное обеспечение**, особое внимание уделяйте исправлению систем безопасности. Разработчики могут самостоятельно обнаруживать бреши в защите и закрывать их.
- **Не используйте один пароль для всех учетных записей**, поскольку это чревато тем, что злоумышленник сможет проникнуть во все ваши учетные записи одним паролем.
- По возможности **используйте двухфакторную аутентификацию,** особенно для наиболее важных ваших аккаунтов. Двухфакторная аутентификация не позволит взломать аккаунт с одним лишь паролем, а потребует использования дополнительного устройства безопасности, к примеру отпечатка пальца, сканера глаза или пароля по SMS.
- В том случае, если у вас возникли подозрения, что ваши данные могли украсть, рекомендуется немедленно сменить все пароли от аккаунтов.



- Мошенники могут попытаться обмануть вас в любой момент, потому нужно **всегда анализировать происходящее, не торопиться с принятием решений.**
- К примеру, если вам звонят неизвестные по телефону никогда не сообщаете никакой личной информации, особенно, если она связана с финансами. В том случае, если вы получаете письмо на электронную почту, не скачивайте сразу приложений из него, а также внимательно читайте все ссылки и описание, поскольку это может быть обманка. БУДЬТЕ БДИТЕЛЬНЫ!

Подготовлено ФУАМО Кимовский район с использованием Интернет- ресурсов,2023

СПАСИБО

ЗА

ВНИМАНИЕ !