ФИШИНГ
И ЕГО ОСНОВНЫЕ ТИПЫ

КОРНЕВА Ж.В.
Начальник Регионального центра финансовой грамотности
ГАДПО ЛО «ИРО»

Наиболее развитой формой мошенничества в Интернете является фишинг - тип киберпреступления, при котором преступники выдают себя за надежный источник, чтобы вынудить жертву передать им личную информацию: имя пользователя, пароль и номер банковской карты и пр.

ЦЕЛЬЮ ЛЮБОГО ФИШИНГОВОГО МОШЕННИЧЕСТВА ЯВЛЯЕТСЯ КРАЖА ЛИЧНОЙ ИНФОРМАЦИИ, ОДНАКО, СУЩЕСТВУЮТ РАЗЛИЧНЫЕ ТИПЫ ФИШИНГА, ЗНАТЬ КОТОРЫЕ НЕОБХОДИМО, ДАБЫ СНИЗИТЬ РИСК ПОПАДАНИЯ В РУКИ МОШЕННИКОВ

1. **ПОЧТОВЫЙ ФИШИНГ.** Будучи самым распространенным типом фишинга, он зачастую использует технику «spray and pray»: хакеры выдают себя за некую легитимную личность или организацию, отправляя массовые электронные письма. Такие письма содержат характер срочности, например, сообщая получателю, что его счет был взломан, а потому он должен срочно ответить. Цель заключается в том, чтобы срочностью вызвать необдуманное действие от жертвы, например, нажать на вредоносную ссылку, которая ведет на поддельную страницу авторизации.
2. **СПЕАРФИШИНГ.** Включает в себя отправку вредоносных электронных писем конкретным лицам внутри конкретной организации. Такие типы писем часто более персонализированы, они заставляют жертв поверить в то, что у них есть отношения с отправителем.
3. **УЭЙЛИНГ.** Вместо того, чтобы преследовать любого сотрудника в компании, мошенники специально нацеливаются на руководителей, например на генерального директора, имеющего доступ к более конфиденциальным данным. Часто такие электронные письма используют ситуацию, способную оказать на руководителей серьезное давление, например, передавая информацию о поданном против компании судебном иске. Такое письмо побуждает получателя перейти по вредоносной ссылке или к зараженному вложению.
4. **SMS-ФИШИНГ.** Для проведения фишинговой атаки использует текстовые сообщения. Принцип действия такой же, как и при осуществлении фишинговых атак по электронной почте: злоумышленник отправляет текстовое сообщение от, казалось бы, легитимного отправителя, которое содержит вредоносную ссылку.
5. **ГОЛОСОВОЙ ФИШИНГ.** Атака проводится с помощью телефонного звонка, который часто передает автоматическое голосовое сообщение, например, от вашего банка, что вы задолжали большую сумму денег, срок действия вашей автостраховки истек или ваша кредитная карта имеет подозрительную активность, что необходимо срочно исправить.