**Что такое фишинг и как от него защититься.**

Фишинг (от англ. fishing — рыбачить, выуживать) — это вид кибератаки, при которой злоумышленник пытается получить доступ к личной информации пользователя, например, к логину и паролю от электронной почты или данным банковской карты.

Фишинг отличается от других видов хакерских атак тем, что мошенники активно манипулируют базовыми человеческими эмоциями, такими как любопытство и страх, а также используют информацию, которые смогли собрать из открытых источников о человеке.

Фишинг проходит по электронной почте, SMS, в мессенджерах и в социальных сетях. Атака выглядит так: человек получает письмо или сообщение от сервисов, которым он доверяет. Например, от своего банка, интернет-провайдера или магазина, где недавно совершил покупку. В этом письме его просят срочно указать личные данные или обновить их, иначе счёт будет заблокирован или возникнут другие проблемы. Это и есть приманка, так называемое «забрасывание удочки».

Важно, что злоумышленники формулируют текст письма исходя из цели привлечения внимания, например: «Ваш аккаунт заблокирован», «Привет, это написано про тебя?», «Отсылаю обещанные фотографии» и т.п.

Для защиты от фишинга важно помнить несколько базовых правил.

**Не отвечайте на подозрительные сообщения**

Фишинговые атаки часто начинаются через электронную почту, сообщения в социальных сетях или мессенджерах. Мошенники используют разные способы, чтобы убедить человека предоставить им личные данные или перевести деньги. Никогда не отвечайте на подозрительные сообщения и не переходите по ссылкам, которые вы не запрашивали.

**Проверьте адрес отправителя**

Мошенники могут подделать адрес отправителя, чтобы сделать письмо более правдоподобным. Однако если вы внимательно посмотрите на него, то обнаружите, что он не соответствует официальному адресу компании. Если сомневаетесь в подлинности письма, обратитесь в службу поддержки компании и уточните информацию.

**Используйте антивирусы и определители номеров**

Антивирусное программное обеспечение помогает защитить компьютер от спам-сообщений, а определитель номеров — от звонков, которые используют для фишинговых атак. Обновляйте своё антивирусное программное обеспечение регулярно, чтобы защитить себя от новых видов угроз.

**Используйте разные пароли для разных сайтов**

Многие люди используют один пароль для всех сервисов. Это удобно, но, насколько бы он ни был сложным, узнав его, злоумышленники смогут авторизоваться на всех сайтах, которыми пользуется человек.

Подготовлено прокуратурой Верховского района.