Фишинг

Узнайте о том, что такое фишинг, как он работает и как его обнаружить.

1. Что такое фишинг?

Фишинг — это мошенничество, цель которого заключается в следующем:

- выманить у вас ценные персональные данные;
- вынудить вас обманом выполнить задачу или действие (например, нажать на ссылку), что позволит установить на ваше устройство вредоносную программу.

В случае утечки данных хакеры зачастую получают такие данные, как адреса электронной почты, после чего они рассылают на эти адреса фишинговые сообщения, пытаясь вас обмануть.

2. Как распознать фишинг?

Попытки фишинга могут осуществляться различными способами:

- электронные письма;
- СМС-сообщения;
- телефонные звонки.

С целью обмана мошенники часто пытаются сыграть на эмоциях и прибегают к различным уловкам. Например:

- **Страх.** В этом случае вам сообщают, что у вас есть задолженность или возникли проблемы, чтобы вызвать у вас панику и вынудить вас сделать то, что от вас требуется.
- **Сочувствие.** В этом случае вам расскажут печальную историю или постараются вызвать у вас сочувствие, чтобы убедить что-то сделать.
- **Возможность или приз.** Вам предложат мнимую возможность (например бесплатную

поездку), чтобы вас обрадовать и убедить что-то сделать.

- **Стандартная задача или запрос.** Этот вид мошенничества может выглядеть как стандартный обычный запрос, например с вашей работы.

3. Как выявить фишинг?

Вот несколько рекомендаций, как соблюдать осторожность и избежать фишинга:

- **Будьте осторожны, нажимая на ссылки или открывая что-либо.**

Не спешите сразу нажимать или открывать то, что кажется вам странным или подозрительным. Ели вы не ожидали что-то получить или если полученная просьба кажется очень срочной или настораживающей, не спешите и выполните проверку, прежде чем что-либо делать.

- **Проверьте отправителя письма и ссылки.**

Выглядит ли адрес электронной почты подлинным? В случае фишинга по электронной почте имя отправителя может выглядеть подлинным, но адрес электронной почты не будет совпадать с именем отправителя. Ссылка также может быть сокращенным URL-адресом или чем-то подозрительным. Проверьте ссылку, наведя на нее указатель мыши. Помните: ни на что не нажимайте, пока не проверите!

- **Проанализируйте запрос.**

Есть ли у вас там вообще учетная запись? Проанализируйте то, о чем вас просят.

- **Обратите внимание на слог запроса.**

Фишинговые сообщения могут содержать необычные обращения (например, «Приветствую, уважаемый!» вместо вашего имени) или странные фразы. Опечатки, грамматические ошибки и другие странности тоже могут указывать на то, что сообщение было отправлено не из подлинной организации. Также обратите внимание на то, чего от вас хотят. Например, подлинные организации не будут запрашивать вашу конфиденциальную информацию по телефону или требовать ваш пароль.

- **Выполните поиск.**

  Очень полезным может оказаться поиск информации о том, чего от вас хотят! Часто можно найти сообщения и статьи об основных распространенных разновидностях фишинга, поэтому поиск может помочь вам убедиться, мошенничество это или нет.

4. Как избежать фишинга?

Обеспечьте защиту паролей и цифровую безопасность!

- Своевременно обновляйте настройки безопасности на ваших устройствах.
- Используйте многофакторную аутентификацию как дополнительный уровень защиты на сайтах, которыми пользуетесь.
- Делайте резервные копии данных.

Надлежащее обеспечение безопасности данных поможет вам сохранить ваши данные и информацию и не стать жертвой фишинга. Но помните, что фишинг становится все более распространенным явлением. Избежать его полностью практически невозможно, поэтому важно уметь его распознавать.

5. Вспомните свой прошлый опыт

С какими видами фишинга вы сталкивались? Запишите здесь, что вы выдели, слышали или с чем сталкивались:

6. Проверьте свои знания и навыки

Проверьте свои навыки и научитесь лучше выявлять попытки фишинга с помощью этого упражнения:

- Проверьте свои навыки с помощью этого теста на фишинг от Google: https://phishingquiz.withgoogle.com/.
- После прохождения теста разбейтесь на небольшие группы и рассмотрите распространенные примеры фишинга на этом сайте: https://www.phishing.org/phishing-examples.
- Подумайте о том, какие тенденции вы заметили и какие методы манипуляции используются в этих примерах.