**Что такое фишинг: как не стать жертвой мошенников?**

Фишинг (англ. phishing) — вид интернет-мошенничества, целью которого является получение идентификационных данных пользователей (логин, пароль, номер кредитной карты и другой конфиденциальной информации), а также запуск вредоносного программного обеспечения на компьютере пользователя.

Такой вид интернет-мошенничества, как правило, основан на психологической манипуляции и его цель - вывести человека на такие эмоции, как интерес, страх, жадность, злость, желание помочь. Это позволяет ослабить концентрацию человека, усыпить его бдительность.

Так, применение различных психологических приемов делает такой вид интернет-мошенничества чрезвычайно эффективным.

Как правило, фишинговая атака представляет собой выдачу фейковых сайтов, имитирующих интернет-страницы популярных компаний: социальных сетей, интернет-магазинов и т.д. Мошенники рассчитывают на то, что пользователь не заметит подделки и укажет на странице личные данные: реквизиты карты, логин и пароль, номер телефона, чем осуществят к получению личных данных.

Основная проблема, связанная с фишингом, заключается в том, что сайты-фейки трудно отличить от оригиналов.

Количество фишинговых атак растет из года в год. Чаще всего подделываются следующие ресурсы: онлайн-сервисы, почтовые сервисы, финансовые учреждения, облачные хранилища, платежные сервисы. Киберпреступники действуют исходя из спроса пользователей на интернет-продукты.

Главной целью фишинга является завладение реквизитами банковских карт, логинами и паролями для входа в аккаунт и т.д.

Самые распространенные типы фишинга:

1) По способу распространения сайты-подделки делят на два типа:

- приходят в рассылке по электронной почте или в мессенджерах;

- выдаются в поиске;

2) По методу сбора данных:

- фейковый сайт;

- вредоносный файл.

Пример. Для злоумышленника не составляет труда найти в открытых источниках информацию о структуре Вашего субъекта, определить ключевых должностных лиц и домен почтовой системы. Это позволяет злоумышленнику сделать фишинговую рассылку примерно следующего содержания: «Уважаемый ....! В период с 1 марта по 3 апреля Управлением информационных технологий производится ревизия почтовых ящиков сотрудников .... Все неиспользуемые почты будут отключены. Если вы получили данное письмо и планируете использовать данный почтовый ящик в будущем, просьба оперативно войти в личный кабинет по следующей ссылке:..........................................».

При этом ссылка, конечно же, ведет на поддельную форму авторизации в почтовую систему. Если тот или иной сотрудник вовремя не поймет, что данная рассылка является фишинговой, и перейдет по ссылке, он окажется на странице, которая внешне неотличима от настоящей формы ввода учетных данных. Конечно же, введя логин и пароль, такой сотрудник «добровольно» передаст их злоумышленникам.

В России ежедневно рассылают до 1 млн сообщений с фейковыми сайтами. Их получают частные лица и организации.

Что делать, чтобы не стать жертвой фишинга?

1. Не переходите по ссылкам, присланным в подозрительных или непонятных сообщениях электронной почты, социальных сетях и мессенджерах.

2. Не загружайте вложенные файлы из сообщений, которых вы не ожидали.

3. Внимательно проанализируйте адрес сайта (URL), на который вы были переадресованы. В большинстве случаев фишинга URL-адрес отличается от оригинального домена одним знаком (например, заканчиваться на .com вместо .gov, или wiLdberries.ru wildberries.ru с заглавной i вместо I).

4. Обновляйте браузер до последней версии.

5. Не совершайте онлайн-покупки по предоплате на непроверенных сайтах.

6. Для покупок в Интернете используйте отдельную банковскую карту.

7. Проверьте домен на сайте tcinet.ru. Там можно узнать дату регистрации: как правило, мошеннические сайты живут несколько дней.

Будьте внимательны и осторожны!