УДК 004.056.5

К ВОПРОСУ О ФИШИНГ-МОШЕННИЧЕСТВАХ В КЕМЕРОВО

А. С. Соловьева, МБОУ «Гимназия № 41», 8 класс
Научный руководитель: Л.П. Селиванова, методист
Кузбасский центр детского и юношеского туризма и экскурсий
г. Кемерово

В современном мире, где интернет прочно вошел в нашу жизнь, угрозы кибербезопасности становятся все более актуальными. Фишинг – одна из наиболее распространенных форм киберпреступлений, представляет собой серьезную опасность для пользователей сети.

Фишинг (от англ. fishing – «рыбалка») - это вид мошенничества, при котором злоумышленники пытаются получить доступ к конфиденциальной информации, такой как пароли, номера кредитных карт или данные банковских счетов, путем обмана пользователей. Для этого они используют поддельные веб-сайты, электронные письма, сообщения в мессенджерах, которые выглядят как настоящие, но на самом деле являются ловушками.

Рассмотрим виды фишинга.

Обман по электронной почте (e-mail фишинг). Злоумышленники отправляют поддельные электронные письма, имитирующие официальные сообщения от банков, интернет-магазинов, социальных сетей или государственных учреждений. Например, поддельные электронные письма от банков: Злоумышленники отправляют письма, маскируясь под Сбербанк, ВТБ, Тинькофф и другие популярные банки. Они могут просить вас обновить данные аккаунта, «подтвердить» подозрительную транзакцию или перейти по ссылке для получения «бонуса».

На слайде вы видите скриншот из электронной почты. Обращаем внимание на имя отправителя, стиль письма и содержание. Письмо пришло с неофициального непонятного адреса, адрес нам неизвестен. Не открываем вложения в подозрительных электронных письмах. Здесь предлагают быстро обогатиться, перейдя по ссылке. Могут предложить очень привлекательные скидки, подарки. На раздумья дают немного времени, поторапливают. В таком случае надо позвонить по официальному телефону компании и уточнить заинтересовавшую информацию.

Обман по СМС (СМС-фишинг). Злоумышленники используют СМС-сообщения для обмана пользователей. Они могут отправлять сообщения с просьбой подтвердить личные данные, перейти по ссылке для получения скидки или приза, а также о блокировке аккаунта, требуя срочно перейти по ссылке для его разблокировки.

Злоумышленники отправляют сообщения, имитирующие СМС от государственных органов, например, Росреестра. Они могут требовать «оплатить

госпошлину», «подтвердить регистрацию» или «отменить» несуществующую операцию.

В данном случае мы не переходим по указанным ссылкам, не звоним по указанным номерам, а обращаемся по официальному телефону организации.

Фишинг с помощью онлайн-объявлений. Мошенники размещают на сайтах объявлений привлекательные предложения, например, «дешевые авиабилеты» или «продаваемые товары по низкой цене». Когда вы переходите по ссылке, попадаете на поддельный сайт, где вас просят ввести личные данные.

Фишинг в социальных сетях. Злоумышленники создают поддельные профили в социальных сетях (VK, Одноклассники) или используют уже существующие профили для обмана пользователей. С таких фейковых или взломанных аккаунтов ведётся переписка, чтобы получить доступ к данным реальных пользователей или заставить перейти по вредоносной ссылке. В данном случае мы обращаем внимание на стиль письменной речи собеседника, на то, как он к нам обращается. При просьбах надо позвонить собеседнику и уточнить детали просьбы.

Телефонный фишинг, социальная инженерия. Злоумышленники используют телефонные звонки, чтобы обмануть пользователей. Они могут представляться сотрудниками банка, страховой компании или государственного учреждения, требуя предоставить личные данные или совершить финансовые операции.

На сайте МВД приводится много примеров подобных обманов. Еженедельно доверчивые кузбассовцы переводят миллионы рублей своих и кредитных средств мошенникам.

Фишинговые атаки актуальны для Кемеровской области и для всей России в целом. В России борьба с фишингом регулируется Федеральным законом «Об информации, информационных технологиях и о защите информации». За нарушение данного закона предусмотрена дисциплинарная, гражданско-правовая, административная или уголовная ответственность.

Рассмотрим основные методы защиты от фишинга:

Не переходим по сомнительным ссылкам.

1. Используем надежные пароли: Создаём сложные пароли, которые включают в себя буквы, цифры и символы. Избегаем использования одного и того же пароля для разных учетных записей.

2. Подключаем двухфакторную аутентификацию. Пользователь вводит код, который отправляется на телефон или электронную почту при каждом входе в систему.

3. Используем антивирусное ПО от кражи данных.

4. Не доверяем информации из неизвестных источников: Не предоставляем личные данные на подозрительных сайтах или по телефону.

5. Регулярно обновляем программное обеспечение с исправлениями безопасности.

Таким образом, фишинг является серьезной угрозой для современного общества. Важно понимать, как работает фишинг, и использовать методы защиты от него.