ТЕМА 6 / 15

Фишинг

Фишинг (англ. phishing от fishing «рыбная ловля, выуживание» и «phony» (обман) — мошенничество с целью кражи денег, данных банковской карты, логинов и паролей от ресурсов пользователя (включая «Госуслуги»), паспортных данных.

Мошенники делают рассылку по электронной почте, SMS или в мессенджерах. Она состоит из мотивирующего текста письма и ссылки или QR-кода на мошеннический ресурс. Выглядят послания как отправленные из компаний, пользующихся доверием.

Фишинг очень распространен. Только за первое полугодие 2021 года россияне пытались пойти по поддельным ссылкам 36 000 000 раз.

Признаки фишинга

- Сообщение о блокировке профиля на другом ресурсе. Указываются причины: взлом пароля, рассылка спама, черный список, нехватка памяти.
- Предложение оплатить со скидкой штраф ГИБДД или другой подобный платеж.
- Письмо с сообщением о задолженности от банка.
- Вызов в арбитражный суд.
- Предложение установить полезную программу, скачать книгу или фильм.
- Сообщение со взломанного аккаунта в соцсетях с просьбой пройти опрос, проголосовать в фотоконкурсе и так далее.
- После перевода общения из официального чата доски объявлений или сервиса знакомств присылают ссылку на платежную систему или с просьбой оплатить билеты на мероприятия для личной встречи.
- Предложение купить популярный товар с большой скидкой на сайте-подделке под известную торговую платформу.
- «Вам положена социальная выплата!».
- Предложение популярных услуг (бронирование гостиниц, турпутевок, благотворительность).
- Выигрыш в лотерею или в конкурсе.
- Просьбы предоставить логин и пароль для помощи в создании антифишинговой защиты.

Что делают фишинговые сайты

- Загружают на устройство пользователя программу-шифровальщик. За ключ к шифру придется добровольно заплатить, или распрощаться с данными навсегда.
- Загружают программу, считывающую нажатия на клавиатуру, или перехватчик паролей. Таким образом мошенники крадут доступ к соцсетям, почте, интернет-банку.
- Переводят на поддельный сайт известного сервиса, которым многие пользуются, и требуют ввести логин и пароль.
- Переводят на сайт поддельной платежной системы. Когда пользователь вводит данные карты для платежа, они уходят мошенникам. Кроме того, преступники могут перехватить и значительно увеличить введенную сумму.

Правила безопасного поведения

- Установите и регулярно обновляйте программу-антивирус с функцией защиты от фишинговых и спам-писем.
- При получении ссылки по электронной почте проверьте адрес отправителя: серьезные компании не делают рассылок с бесплатных почтовых сервисов. Если поле «Отправитель» не заполнено, это наверняка массовая фишинговая рассылка.
- Не открывайте вложения и не переходите по ссылкам от неизвестных отправителей.
- Даже если источник доверенный, тщательно проверьте адрес: он должен полностью совпадать с адресом официального ресурса, который можно найти через поисковик.
- Подключите оповещения об операциях с банковской картой.
- Пользуйтесь браузерами Chrome, Safari и Firefox: у них есть встроенная антифишинговая защита.
- Подключите подтверждение платежа по паролю, который банк присылает в SMS.
- Установите двухфакторную аутентификацию (по коду из SMS) на все ресурсы, которые позволяют это сделать, и в первую очередь – на «Госуслуги».

- Сообщайте о подозрительных электронных письмах своей службе информационной безопасности, а при использовании бесплатных сервисов обязательно отмечайте фишинговые письма как спам. Открывать их для этого необязательно.
- Рассчитывайтесь в интернете со специальной карты (можно завести для этого виртуальную). Деньги на нее перечисляйте в том объеме, который необходим для конкретного платежа.
- Проверяйте просьбы о помощи от друзей, связавшись с ними через другой канал (лучше по телефону), а предложения сверхвыгодных покупок – на официальном сайте компании.
- Если сайт требует ввести персональные данные, он должен работать по защищенному соединению https. Это обозначается значком закрытого замка слева от адресной строки.

Что делать, если перешел на фишинговый сайт?

Обязательно сообщите в полицию. Это поможет остановить мошенников.