

Шесть эмоциональных крючков, которыми пользуются мошенники



Страх

Все мы чего-то боимся. Есть страхи очевидные — потеря близких или чего-то ценного (жилья, денег, привилегий и так далее). Эти страхи активно используются в мошеннических схемах.

Есть неочевидные — об этих страхах злоумышленники могут узнать, если поделиться ими в публичном пространстве: соцсетях, мессенджерах или интервью.

Примеры сообщений:

«Защити свои сбережения — переведи их на резервный счет»,

«Ваш личный кабинет будет заблокирован — срочно поменяйте пароль»,

«Поможем отмазаться от мобилизации»,

«Вы внесены в базу должников ФССП, и вам будет ограничен выезд за границу».



Раздражение

Вас могут забрасывать бесконечными спам-сообщениями, в которых будет кнопка, картинка или ссылка, позволяющая от них отписаться.

Это — один из любимых методов мошенников. Вместо страницы отписки откроется фишинговый ресурс либо начнется загрузка вредоносного ПО на устройство.



Любопытство

Представьте, что после вечеринки, где вы хорошо провели время, вам приходит сообщение: «Смотри в видосе по ссылке, как ты отжигашь». Конечно, интересно проверить, не станете ли вы очередной «звездой ютьюба». Только сначала нужно «обновить плеер». Вы соглашаетесь... и загружаете на свой девайс вредоносное ПО.

В эпидемию COVID-19 по такой же схеме отправлялись ссылки с «секретными картами заражения» и «реальным числом заболевших».

Примеры сообщений:

«Узнай истинное число зараженных COVID-19»,

«Хочешь узнать способ увеличения своего дохода в три раза без усилий и за две недели?»,

«Все звезды худеют, используя это средство...».



Жадность

Еще одно свойство человека — желание получить больше при минимуме вложенных усилий.

Поэтому так сложно отказаться, когда вам предлагают что-либо купить или оформить подписку в десять раз дешевле. Так мошенники могут получить доступ к вашим платежным или учетным данным или заставить вас совершить какие-либо действия во вред себе.

Примеры сообщений:

«Получи доступ к онлайн-кинотеатру с тысячами фильмов бесплатно»,

«Вы выиграли автомобиль»,

«Купи билеты в Таиланд со скидкой в 90%»,

«Российская Федерация прощает все долги до 2022-го года».



Желание помочь

Оказать помощь в виртуальном пространстве, переведя деньги в благотворительный фонд или поучаствовав в сборе средств, гораздо проще, чем, к примеру, поехать куда-либо в качестве волонтера.

Поэтому люди часто откликаются на такие призывы — которые могут исходить от мошенников. Возможно, вы просто переведете деньги злоумышленникам, а возможно, они получат еще и данные вашей карты, если перевод будет проходить через форму на сайте.

Примеры сообщений:

«Сбор средств на приют для бездомных животных»,

«Сбор средств в помощь пострадавшим от наводнений»,

«Помогите Лизе, потерявшей родителей»,

«Проголосуй за моего ребенка».



Невнимательность

Люди часто делают опечатки или не обращают внимания на слова, которые исказила функция автонабора.

Мошенники пользуются этим и размещают свои ресурсы на сайтах, отличающихся от нужных и знакомых вам буквально на одну-две буквы. Таким образом случайное нажатие на соседнюю клавишу может привести вас вместо сайта знакомого банка на сайт онлайн-казино или на фишинговый кредитный ресурс.

Примеры фишинговых ресурсов

cberbank[.]ru,

sberbamk[.]ru,

gismete0[.]ru,

onetimesercet[.]com.

