Ежемесячный информационный бюллетень по безопасности

Мошенничество с благотворительностью и стихийными бедствиями

Киберпреступники знают, что один из лучших способов подтолкнуть людей к совершению ошибки — создать повышенное чувство срочности. И один из самых простых способов создать ощущение срочности — воспользоваться кризисом. Вот почему киберпреступники используют это всякий раз, когда происходит серьезное событие с глобальными последствиями. То, что большинство из нас считает трагедией, киберпреступники рассматривают как возможность, например, начало войны, крупное стихийное бедствие, такое как извержение вулкана, и, конечно же, вспышки инфекционных заболеваний, таких как COVID-19. Когда об определенном событии появляется огромное количество сообщений в социальных сетях и новостях, киберпреступники понимают, что пришло время нанести удар.

Они используют эту возможность для создания своевременных фишинговых писем или мошеннических сообщений, а затем отправляют это фишинговое письмо или запускают аферу миллионам людей по всему миру. Например, во время стихийного бедствия они могут притвориться благотворительной организацией, прося пожертвования для спасения нуждающихся детей. Киберпреступники часто могут действовать в течение нескольких часов после кризиса или стихийного бедствия, поскольку вся техническая инфраструктура у них подготовлена. Как мы можем защитить себя в следующий раз, когда произойдет большой кризис или катастрофа, и киберпреступники попытаются этим воспользоваться?

Как обнаружить и защититься от мошенников

Ключом к тому, чтобы избежать мошенников, является подозрительное отношение к любому, кто обращается к вам. Например, не доверяйте срочному электронному письму, в котором утверждается, что оно отправлено благотворительной организацией, которая остро нуждается в пожертвованиях, даже если электронное письмо отправлено брендом, который вы знаете и которому доверяете. Не доверяйте телефонному звонку, в котором утверждается, что местная благотворительная организация оказывает на вас давление с целью сделать пожертвование. Чем больше ощущение срочности, тем больше вероятность того, что это атака. Вот некоторые из наиболее распространенных признаков мошенничества с благотворительностью.

- С подозрением относитесь к любой благотворительности, которая требует от вас пожертвований через криптовалюту, Western Union, денежные переводы или подарочные карты.
- Киберпреступники могут изменить номер своего идентификатора вызывающего абонента, чтобы их телефонный звонок выглядел так, как будто он исходит от вашего местного кода или от надежного имени. В наши дни нельзя полагаться на идентификатор вызывающего абонента.
- Некоторые киберпреступники будут использовать имена и логотипы, которые звучат или выглядят как настоящая благотворительность. Это одна из причин, по которой стоит провести некоторое исследование, прежде чем жертвовать.
- Киберпреступники часто делают много расплывчатых и сентиментальных заявлений о том, что они будут делать с вашими деньгами, но не сообщают подробностей о том, как ваше пожертвование будет использовано.

© SANS Institute 2022

- Не думайте, что просьбы о помощи на сайтах краудфандинга, таких как GoFundMe, или на сайтах социальных сетей, таких как TikTok, являются законными, особенно после кризиса или трагедии.
- Некоторые киберпреступники могут попытаться обманом заставить вас сделать им пожертвование, поблагодарив вас за пожертвование, которое вы сделали в прошлом, когда на самом деле вы никогда этого не делали.
- Не разглашайте личную или финансовую информацию в ответ на любой незапрашиваемый запрос.

Как изменить ситуацию безопасно

Чтобы сделать пожертвование в трудную минуту или помочь пострадавшим от стихийного бедствия, делайте пожертвования только известным и надежным организациям. Вы устанавливаете связи и решаете, к кому обратиться, например, какие веб-сайты посетить или в какие организации позвонить. Когда вы думаете о пожертвовании на благотворительность, ищите его название, а также такие слова, как «жалоба», «отзыв», «рейтинг» или «мошенничество». Не знаете, каким благотворительным фондам доверять? Начните с изучения правительственных веб-сайтов, которым вы доверяете, или, возможно, ссылок, предоставленных известной и пользующейся большим доверием новостной организацией. Пожертвование в трудную минуту — это фантастический способ изменить мир к лучшему, просто убедитесь, что вы жертвуете законным организациям.

Приглашенный редактор

Доктор Джессика Баркер отмеченный наградами лидер в области кибербезопасности. Она является со-генеральным директором Cygenta и автором бестселлеров. Джессика входит в консультативный совет SANS Security Awareness Summit.

Ресурсы

Благотворительное мошенничество FTC: https://consumer.ftc.gov/features/how-donate-wisely-and-avoid-charity-scams
Социальный инжиниринг: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Три главных мошенничества: https://www.sans.org/newsletters/ouch/top-three-social-media-scams/
Текстовые сообщения /SMS фишинг: https://www.sans.org/newsletters/ouch/spot-and-stop-messaging-attacks/
Вишинг - атаки на телефонные звонки и мошенничество: https://www.sans.org/newsletters/ouch/vishing/
Навигатор по благотворительности: https://www.charitynavigator.org/

Роман Полаков

OUCH! Публикуется SANS Security Awareness и распространяется под лицензией Creative Commons BY-NC-ND 4.0. Вы можете делиться или распространять этот информационный бюллетень, если вы не продаете и не модифицируете его. Редакционная коллегия: Уолтер Скривенс, Фил Хоффман, Алан Ваггонер, Лесли Ридаут, Принцесса Янг.