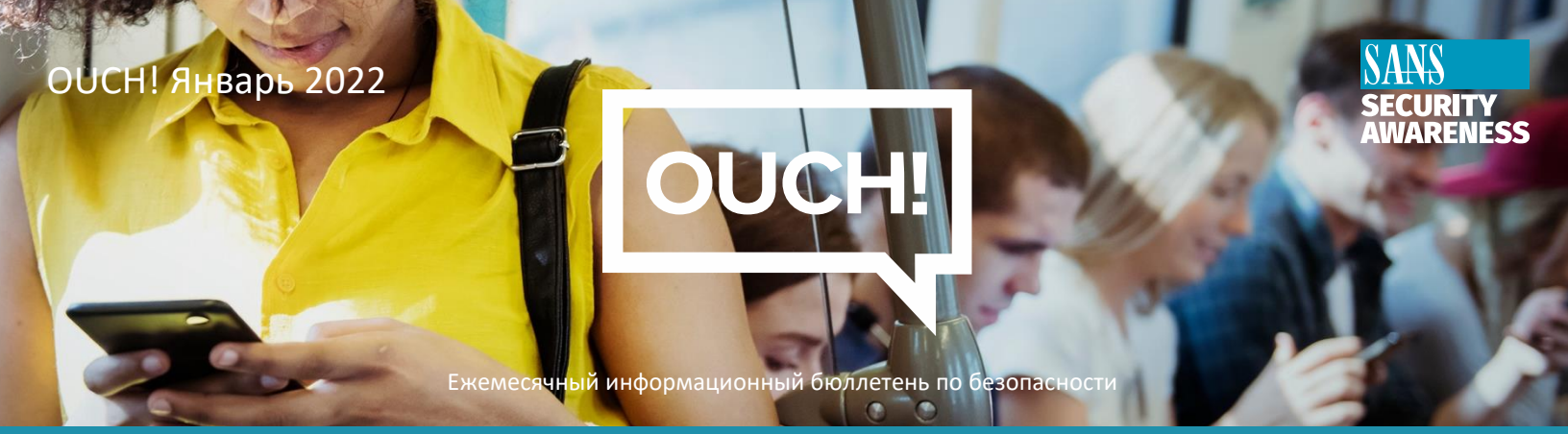
OUCH! Январь 2022



Ежемесячный информационный бюллетень по безопасности

# Обнаружение и прекращение атак с помощью текстовых сообщений

## Как происходят атаки с помощью текстовых сообщений?

Smishing (слово-портмоне, объединяющее SMS и фишинг) - это атаки, которые происходят, когда кибер-злоумышленники используют текстовые сообщения или аналогичные технологии обмена сообщениями, чтобы заставить вас предпринять действия, которые вы не должны предпринимать. Возможно, они обманом заставят вас предоставить данные вашей кредитной карты, заставят позвонить по номеру телефона, чтобы получить вашу банковскую информацию, или убедят вас заполнить онлайн-опрос для сбора вашей личной информации. Как и в случае с фишинговыми атаками по электронной почте, киберпреступники часто играют на ваших эмоциях, чтобы заставить вас действовать, например, вызывая чувство срочности или любопытства. Однако то, что делает атаки с использованием обмена сообщениями настолько опасными, заключается в том, что в тексте гораздо меньше информации и меньше подсказок, чем в электронном письме, что значительно усложняет обнаружение того, что что-то не так.

Распространенное мошенничество - это сообщение о том, что вы выиграли iPhone, и вам нужно только щелкнуть ссылку и заполнить опрос, чтобы получить его. На самом деле телефона нет, и опрос предназначен для сбора вашей личной информации. Другим примером может быть сообщение о том, что посылка не может быть доставлена со ссылкой на веб-сайт, где вас просят предоставить информацию, необходимую для завершения доставки, включая данные вашей кредитной карты для покрытия «платы за обслуживание». В некоторых случаях эти сайты могут даже попросить вас установить неавторизованное мобильное приложение, которое заражает ваше устройство и захватывает его.

Иногда киберпреступники даже комбинируют атаки по телефону и с помощью обмена сообщениями. Например, вы можете получить срочное текстовое сообщение от банка с вопросом, разрешаете ли вы тот или иной платеж. В сообщении вас попросят ответить ДА или НЕТ для подтверждения платежа. Если вы ответите, киберпреступник теперь знает, что вы готовы к сотрудничеству, и позвонит вам, представившись отделом безопасности банка. Затем они попытаются узнать у вас информацию о вашей финансовой и кредитной карте или даже о логине и пароле вашего банковского счета.

## Обнаружение и остановка атак с использованием текстовых сообщений

Вот несколько вопросов, которые стоит задать себе, чтобы определить наиболее распространенные виды атак с использованием текстовых сообщений:

- Огромное чувство срочности, когда кто-то пытается торопить вас, чтобы совершить действие.
- Переносит ли сообщение вас на веб-сайты, которые запрашивают вашу личную информацию, кредитную карту, пароли или другую конфиденциальную информацию, к которой у них не должно быть доступа?
- Звучит ли сообщение слишком хорошо, чтобы быть правдой? Нет, вы действительно не выиграли новый iPhone.
- Вынуждает ли сссылка на веб-сайт или сервис платить нестандартными методами, такими как биткойны, подарочные карты или переводы Western Union?
- В сообщении запрашивается код многофакторной аутентификации, который был отправлен на ваш телефон или сгенерирован вашим банковским приложением?
- Сообщение похоже на «неправильный номер»? В таком случае не отвечайте на него и не пытайтесь связаться с отправителем; просто удали его.

Если вы получили сообщение от официальной организации, которое вас насторожило, свяжитесь с ними напрямую. Не используйте номер телефона, указанный в сообщении, вместо этого используйте надежный номер телефона. Например, если вы получили текстовое сообщение от вашего банка, в котором говорится, что проблема с вашим банковским счетом или кредитной картой, обратитесь в банк или компанию-эмитент кредитных карт, посетив их веб-сайт или позвонив напрямую по номеру телефона, указанному на задней части банковской карты. Также помните, что большинство государственных органов, таких как налоговые или правоохранительные органы, никогда не свяжутся с вами через текстовое сообщение, они будут связываться с вами только по почте.

Когда дело доходит до атак с помощью текстовых сообщений, вы - ваша лучшая защита.

## Приглашенный редактор

Джефф Ломас - детектив группы кибер-расследований столичного департамента полиции Лас-Вегаса и преподает курс SANS SEC487 «Сбор и анализ разведывательной информации с открытым исходным кодом» (OSINT). Джефф расследует высокотехнологичные финансовые преступления, в том числе компрометацию деловой электронной почты, SMS атаки, программы-вымогатели, а также сложные дела о краже криптовалюты и отмывании денег.

## Ресурсы

**Предотвратить атаки по типу фишинга:** https://www.sans.org/newsletters/ouch/stop-that-phish/
**Социальный инжиниринг:** https://www.sans.org/newsletters/ouch/social-engineering-attacks/
**Вишинг - атаки по телефону:** https://www.sans.org/newsletters/ouch/vishing/

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