Ежемесячный журнал по вопросам компьютерной безопасности

OUCH!

**В ЭТОМ ВЫПУСКЕ…**

- **Что такое целевой фишинг**
- **Эффективность целевого фишинга**
- **Как себя защитить**

# Целевой Фишинг

## Что такое целевой фишинг

Вы, скорее всего, знаете, что такое фишинг атаки: кибермошенники рассылают электронные письма миллионам потенциальных жертв. Эти сообщения специально созданы для обмана или нападения. Обычно такие письма похожи на письма от достоверных источников, например, вашего банка или знакомых. В таких письмах часто создается иллюзия срочности или слишком хорошего предложения для вас. Если вы перейдёте по ссылке, то попадёте на зараженный вирусами сайт, который попытается взломать ваш компьютер или похитить логин и пароль. Часто такие письма содержат инфицированные вложения, которые при открытии заражают вирусом и злоумышленники получают контроль над вашим компьютером. Такого рода письма мошенники стараются отправить максимально возможному количеству людей. Чем больше людей получат письма, тем больше вероятность найти жертву.

**Об авторе**

Ленни Зельцер – автор июльского выпуска OUCH! Ленни специализируется на защите клиентов в сфере IT корпорации NCR и читает лекции по борьбе с вирусами в институте SANS. У Ленни есть страничка в Twitter **@lennyzeltser** и блог **blog.zeltser.com**

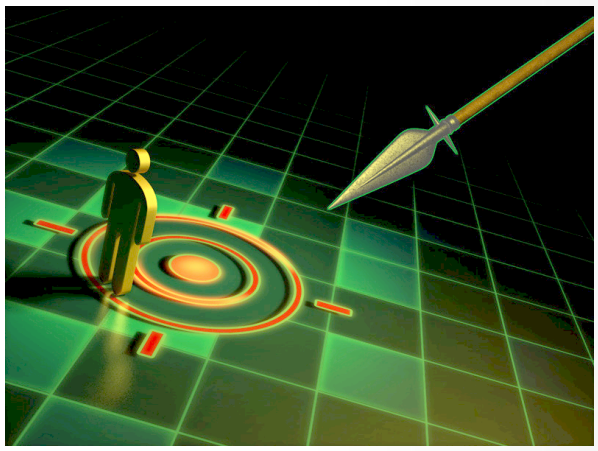
Есть более эффективный способ атаки, относительно новый тип, так называемый целевой фишинг. Принцип такой же, киберпреступники рассылают электронные письма потенциальным жертвам от имени организаций или людей, которым доверяют. Однако, в отличие от обычного фишинга, целевой фишинг точно ориентирован. Вместо рассылки миллионов писем потенциальным жертвам, киберпреступники отправляют небольшое количество писем заранее выбранным людям, например, 5-10 жертвам. В отличие от обычного фишинга, для целевого фишинга преступники проводят тщательную подготовку, например, просматривают страницы жертвы на LinkedIn или Facebook или другие записи в блогах или форумах. На основе полученной информации, мошенники создают индивидуальное электронное письмо, которое соответствует намеченным целям. В этом случае у мошенников больше шансов обмануть потенциальную жертву.

## Эффективность целевого фишинга

Целевой фишинг используется в тех случаях, когда мошенники собираются атаковать именно вас или вашу компанию. В отличие от обычных мошенников, которые просто хотят похитить деньги, мошенники, которые используют целевой фишинг, преследуют очень специфические цели, обычно хотят получить

# Целевой Фишинг

конфиденциальную информацию, например, корпоративные бизнес секреты, разработки в сфере высоких технологий или конфиденциальную правительственную информацию. Возможно, вашу компанию хотят использовать как трамплин для получения доступа к другой компании. Такие нападающие готовы тратить много времени и усилий для достижения своих целей.



*Лучший способ защиты от целевого фишинга – не стать интересной целью: ограничьте информацию, которую публикуете о себе, и сообщайте о подозрительных письмах.*

Например, иностранное правительство решает, что ваша компания разработала продукт или технологию, которая является ключевой для их экономического развития, и вы становитесь целью. Изучив сайт вашей организации, выбирают три ключевых личности. Затем мошенники изучают страницы этих людей на LinkedIn, Twitter и Facebook и создают досье. После тщательного изучения полученной информации, злоумышленники создают письмо для целевого фишинга от имени поставщика, с которым сотрудничает компания. Письмо содержит зараженное вложение, похожее на счет от поставщика. В итоге двоих человек из трех потенциальных жертв удалось обмануть с помощью целевого фишинга и они открыли заражённое вложение, предоставив иностранному правительству полный доступ к компьютерам, в конечном итоге, ко всем секретным продуктам компании, которые они теперь могут производить и сами.

Целевой фишинг гораздо опаснее обычного фишинга, так как злоумышленники разрабатывают особые способы атаки для вас или вашей компании. Это не только увеличивает шансы на успех нападающих, но и эти атаки гораздо сложней обнаружить.

## Как себя защитить

Первый шаг для защиты от целевых атак – это понимание того, что вы можете стать целью. Прежде всего, вы и ваша компания, скорее всего, обладаете конфиденциальной информацией, которая может заинтересовать ещё кого-нибудь, или быть использована для доступа к другой компании, которая является конечной целью нападающих. Как только вы поймёте, что можете стать целью для атаки, примите следующие меры для защиты себя и своей компании:

## Целевой Фишинг

- Ограничьте информацию о себе, которую публикуете на форумах, Facebook или LinkedIn. Чем больше персональной информации вы публикуете, тем проще кибермошенникам подготовить целевую атаку и создать письмо, похожее на настоящее.

- Если в письме вас просят открыть вложение, перейти по ссылке или запрашивают конфиденциальные данные, проверьте это письмо. Если письмо отправлено от имени компании или человека, которого вы знаете, используйте для связи с отправителем уже имеющиеся контакты, чтобы убедиться в достоверности этого письма.

- Поддерживайте безопасность компании и следуйте политикам безопасности, используйте средства безопасности, например, антивирус, шифрование и обновления, которые вам доступны.

- Помните, что ни одна технология не может полностью предотвратить атаки по электронной почте, особенно целевой фишинг. Если на первый взгляд письмо кажется подозрительным, прочтите его внимательней. Если вы обеспокоены тем, что это целевой фишинг или уже стали жертвой атаки, немедленно свяжитесь со службой поддержки или сотрудниками департамента информационной безопасности.

## Узнайте Больше

Подпишитесь на OUCH! – ежемесячный журнал по информационной безопасности, получите доступ к архивам OUCH! и узнайте больше о решениях SANS в вопросах информационной безопасности на нашем сайте http://www.securingthehuman.org.

## Дополнительная информация

Как не стать жертвой целевого фишинга: http://www.theatlanticwire.com/technology/2013/02/spear-phishing-security-advice/62304/

Как избежать атаки социальной инженерии и фишинг атаки: http://www.us-cert.gov/ncas/tips/st04-014

Целевой фишинг: афера, а не спорт: http://ru.norton.com/spear-phishing-scam-not-sport/article

Фишинговые методы: сходства, различия и тенденции. Часть вторая: целевой фишинг: http://www.securitylab.ru/analytics/440663.php

Фишинг: http://www.securingthehuman.org/resources/newsletters/ouch/2013#february2013

Соварь терминов по информационной безопасности: http://www.securingthehuman.org/resources/security-terms

Ежедневные советы Института SANS: https://www.sans.org/tip_of_the_day.php



Редакция: Билл Уайман, Уолт Скривенс, Фил Хоффман, Боб Рудис
Русский перевод: Александр Котков, Ирина Коткова