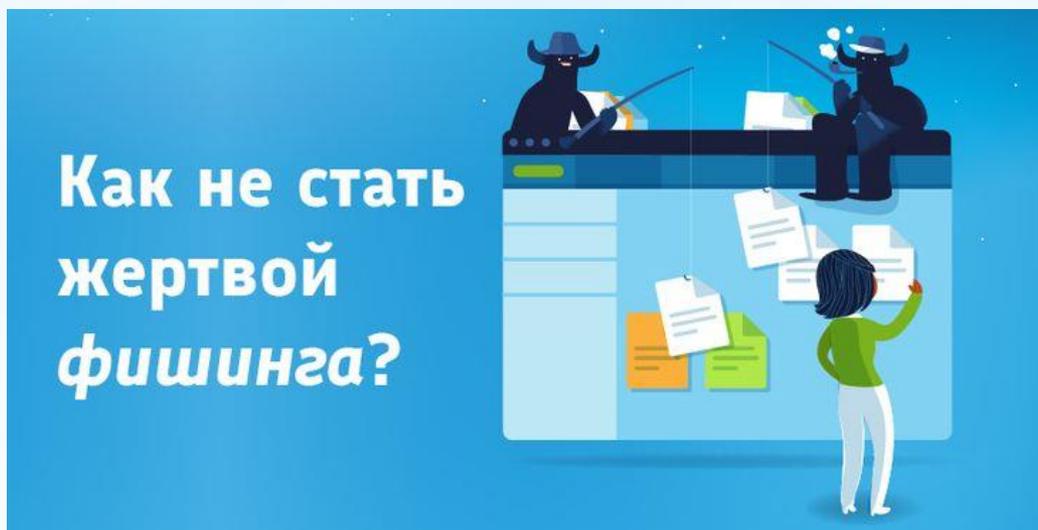


Одним из наиболее опасных видов киберугроз, по словам специалистов, остается фишинг



Жертвами мошенников становятся и обычные пользователи, и организации, а современные средства защиты не всегда способны противостоять меняющейся тактике злоумышленников, так как их механизмы основаны не на технических уязвимостях, а на человеческих слабостях и доверчивости пользователей. О том, что такое фишинг, и способах защиты от него рассказываем в наших карточках.

Что такое фишинг?

Фишинг (от англ. fishing — рыбалка) — вид интернет-мошенничества, цель которого — получить конфиденциальные данные пользователей от них самих. Сюда относится кража паролей, номеров кредитных карт, банковских счетов и другой конфиденциальной информации. Наиболее частые жертвы фишинга — сотрудники банков, электронных платежных систем, онлайн-аукционов.

Фишеров интересуют данные, которые дают прямой доступ к деньгам, а также личная информация пользователей, помогающая сделать достоверными фишинговые письма.

Виды фишинговых приманок

Подделка домена или имитация знакомого пользователя — сообщение может прийти с адреса знакомого вам отправителя или организации, который отличается от исходного какой-нибудь едва заметной деталью или символом (exarmlе@mail.com вместо example@mail.com).

Текстовые приманки — текстовое сообщение, поступающее от якобы доверенного источника, такого как банк, государственное учреждение или коммерческая компания. В сообщении пользователя просят предоставить личную информацию (имя пользователя, пароль или конфиденциальные финансовые данные). Изучите внимательно подобное письмо. Если информация требуется "срочно" или "в кратчайшие сроки" — это один из признаков фишингового письма.

Виды фишинговых приманок

Фишинговые ссылки — сообщение электронной почты содержит ссылку на страницу, похожую на страницу авторизации доверенного сайта и призывающую, например, срочно поменять пароль. Этим действием вы можете передать его непосредственно в руки злоумышленников.

Фишинговые вложения — сообщение электронной почты, которое содержит вредоносный файл, а также некий призыв, убеждающий его открыть.

Псевдовикторины — ресурсы в соцсетях и мессенджерах, которые имитируют розыгрыши ценных призов, крупных денежных сумм или колоссальные скидки на продукцию известных брендов. Применительно к России это особенно касается товаров марок, покинувших местный рынок.

Фишинг или вишинг?

Практически каждый обладатель мобильного телефона на сегодня хотя бы раз сталкивался с разновидностью фишинга, получившей название "вишинг", от англ. voice fishing (голосовой фишинг).

Мошенники звонят жертве, представляясь различными официальными лицами (в основном представителями силовых ведомств или сотрудниками кредитных организаций), выманивая персональные данные, пароли или напрямую деньги.



