

Фишинг: как злоумышленники крадут ваши данные и как от этого защититься

Фишинг — это форма интернет-мошенничества, нацеленная на кражу личных данных пользователей: паролей, логинов, данных банковских карт, паспортной информации. Злоумышленники не взламывают защиту технически, они «взламывают» человека, используя методы социальной инженерии. Их главное оружие — манипуляция эмоциями: страхом, жадностью, любопытством или желанием помочь.

Фишинговые сообщения могут:

- содержат ссылки на внешние ресурсы (особенно короткие ссылки);
- содержать вложения (документы, архивы, презентации могут содержать вредоносный код);
- требовать немедленных действий или вызывают сильные эмоции («Ваш счет блокируют!», «Вы выиграли приз!», «Срочно подтвердите данные!»);
- содержать орфографические и грамматические ошибки;
- касаться финансов, банковских переводов или актуальных событий.

При получении подозрительного сообщения:

1. Проверьте адрес отправителя.
2. Не открывайте подозрительные вложения. Если вы не ждали файл от этого человека или причина его отправки выглядит подозрительной — никогда не открывайте вложение.
3. Используйте «внешний» канал связи. Если сомнения остались, свяжитесь с отправителем по телефону или через мессенджер, используя контакты, которые вы знаете или нашли на официальном сайте. Не звоните по номерам из подозрительного письма.

Что делать, если вы уже стали жертвой фишинга. Если вы передали мошенникам свои данные (ввели их в предложенную форму на подозрительном сайте), то:

1. Позвонить в банк и заблокировать карту, если вы вводили её реквизиты.
2. Срочно сменить пароль скомпрометированного аккаунта и всех сервисов, где вы использовали этот же (или похожий) пароль.
3. Включить двухфакторную аутентификацию (2FA) там, где это возможно. Оптимальный способ — код из приложения-аутентификатора, а не SMS.
4. Проверить активные сессии в важных аккаунтах (почта, соцсети, Госуслуги) и завершить все подозрительные входы.
5. Предупредить близких, если взломали ваш мессенджер или соцсеть, чтобы мошенники не обманули их от вашего имени.
6. Обратиться в правоохранительные органы с заявлением о мошенничестве.

Чтобы не стать жертвой фишинга, достаточно соблюдать несколько простых правил:

- никогда не переходите по ссылкам из подозрительных писем и сообщений;
- всегда проверяйте адрес сайта в строке браузера — если там лишние символы или опечатки, это ловушка;
- не сообщайте никому по телефону или в интернете свои паспортные данные, реквизиты банковских карт и коды из СМС;
- создавайте уникальные сложные пароли для каждого сервиса;
- будьте особенно бдительны в праздничные дни — в периоды повышенного спроса число фишинговых атак увеличивается вдвое .

Помощник прокурора Рыльского района

Д.Г.Довнар