

Прокуратура г. Каменска-Уральского разъясняет

Фишинг как вид интернет-мошенничества

Фишинг является одним из самых распространённых способов интернет-мошенничества.

Как это работает?

Злоумышленники создают поддельные сайты, письма или сообщения, похожие на официальные: от банка, государственного учреждения или известной компании. В них содержится просьба перейти по ссылке, ввести личные данные или подтвердить операцию. Как правило, ссылку присылают по электронной почте, SMS либо в мессенджере. Затем введенные данные попадают к злоумышленникам, которые в последующем используют их для кражи денег или взлома Ваших аккаунтов.

Как можно распознать фишинг:

1. Неверный адрес сайта (например, замена латинской буквы на похожую кириллическую или добавление лишних символов).
2. Отсутствие значка безопасного соединения (замочка) в адресной строке.
3. Ошибки в тексте, устаревший дизайн.
4. Просьба срочно совершить какие-либо действия под угрозой потери средств («подтвердить операцию», «заблокировать аккаунт»).

Кроме того, существуют следующие часто встречающиеся разновидности фишинга:

1. Вишинг — это фишинг по телефону или в мессенджерах. Злоумышленник звонит Вам, представляясь сотрудником банка или государственного органа.
2. Смишинг — аналогичная атака через SMS.
3. Клон-фишинг — мошенники копируют реальное письмо от Вашего знакомого, заменяя в нём ссылку или вложение.