КАК ОБЕЗОПАСИТЬ СЕБЯ ОТ ФИШИНГОВЫХ СООБЩЕНИЙ В МЕССЕНДЖЕРАХ.

Сообщения в социальных сетях и мессенджерах вызывают у людей большее доверие. Этим пользуются злоумышленники, выманивая персональные данные и деньги.

Например, по ссылке в Telegram-канале человек перейдет не задумываясь, тогда как такая же ссылка, полученная по электронной почте, вызовет настороженность.

ДЛЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ И ДЕНЕЖНЫХ СРЕДСТВ РЕКОМЕНДУЕМ:

— УСТАНОВИТЕ АНТИВИРУС

Он умеет распознавать фишинг и недоверенные ресурсы. Регулярно обновляйте базы, без этого антивирус не будет эффективен.

— ПРОВЕРЯЙТЕ ПРИСЛАННЫЕ URL-ССЫЛКИ

Прежде чем перейти по ссылке, проверьте ее безопасность с помощью бесплатных сервисов, например, VirusTotal или Национальный мультисканер.

— НЕ ПЕРЕХОДИТЕ ПО АКТИВНЫМ ССЫЛКАМ

Если в письме или мессенджере вам прислали ссылку на сайт, по которой можно кликнуть, то не делайте этого, она может быть опасной. Лучше найти адрес сайта через поисковик.

— ЧИТАЙТЕ ПРЕДУПРЕЖДЕНИЯ

Если браузер или антивирус три перехоле на сайт сообщают, что этот сайт опасный, лучше по ссылке не переходить.

— ДУМАЙТЕ, ГДЕ ВВОДИТЬ ДАННЫЕ

Оставляйте учетные данные и платежные реквизиты только после того, как убедитесь, что сайту можно доверять.

— ПОМНИТЕ О ЦИФРОВОЙ ГИГИЕНЕ

Не сообщайте никому конфиденциальные данные, используйте надежные пароли, подключайте, где возможно, двухфакторную аутентификацию, делайте резервные копии.

— ВЫГЛЯДИТ ПОДОЗРИТЕЛЬНО - СПРОСИ

Если знакомый прислал странное письмо или сообщение в мессенджере, уточните другим способом связи, действительно ли он его отправлял.

— НЕ ГОНИТЕСЬ ЗА БЕСПЛАТНЫМ СЫРОМ

Сообщения о неожиданных выигрышах, подарках от онлайн-магазина или банка чаще всего рассылают мошенники. Такие сообщения могут содержать вредоносные вложения или фишинговые ссылки.

#МВД #МВД74 #Полиция74 #Челябинскаяобласть #МВДРоссии #ПолицияКатавИвановск #НеДайСебяОбмануть #Будьтебдительны