КАК НЕ СТАТЬ ЖЕРТВОЙ КИБЕРПРЕСТУПЛЕНИЯ?

Прочитайте сами и ознакомьте родных и близких, друзей и знакомых!

Чтобы не стать жертвой преступления, которое совершается с использованием информационных технологий, каждому из нас необходимо выработать очень важную привычку – быть бдительными во всем, в том числе, в нашей личной безопасности и безопасности финансовых средств:

1. Выяснить, что входит в понятие “персональные данные”

2. В каком объеме и на каких ресурсах Вы размещаете данные

3. Могут ли они оказаться в свободном доступе? Нужно ли это Вам?

ОБЩЕСТВЕННЫЙ СОВЕТ ПРИ ГЛАВНОМ УПРАВЛЕНИИ МВД РОССИИ ПО СВЕРДЛОВСКОЙ ОБЛАСТИ

Необходимо критически относиться к любой информации, которую получаете из разных каналов связи - будь то SMS-сообщения или иные сообщения в различных мессенджерах, или звонок, совершаемый посредством телефонной связи или интернет телефонии.

Старайтесь проверить те данные, которые стали Вам известны прежде, чем слепо следовать тем советам, которые были направлены. Сохраняйте спокойствие, трезво оцените ситуацию и незамедлительно проверьте информацию на предмет соответствия действительности. Только в этом случае возможно пресечь действия злоумышленников на начальном этапе их преступного посягательства.

Дополнительно с конкретными примерами возможных сценариев и мер противодействия различным видам преступлений, совершаемым с использованием информационных технологий, можно ознакомиться на официальных ресурсах Федеральных органов исполнительной власти Российской Федерации:

Министерство внутренних дел Российской Федерации:
https://xn--b1aew.xn--p1ai/document/1910260
Федеральная служба по надзору в сфере защиты прав потребителей и благополучие человека (Роспотребнадзор):
https://rospotrebnadzor.ru/activities/recommendations/details.php?ELEMENT_ID=8168

СОВЕТ ДЛЯ РОДИТЕЛЕЙ

Используйте функцию родительского контроля, а также проводите беседы с детьми по вопросам поведения в сети Интернет.

Важно знать об использовании злоумышленниками в сети Интернет груминга: установления доверительных отношений с детьми с целью последующего манипулирования ими и превращения в жертв. Также данное явление проявляется и в кибертравле и кибердомогательстве, которым в особенности подвержены дети.

ОБЩИЙ ВЫВОД

Внимательно проверяйте и контролируйте входящие телефонные звонки на предмет телефонных мошенников при попытках получения доступа к Вашим персональным данным.

Это также касается и интернет-покупок с помощью банковской карты посредством электронных платежей. Рекомендуется проверить сайт на наличие на нем официальных отзывов других клиентов о покупках товаров, а лучше связаться по телефону с продавцами, чтобы удостовериться, что это, действительно, реальные люди и вас не хотят обмануть.