КАК ОБМАНЫВАЮТ В ИНТЕРНЕТЕ

НАЦИОНАЛЬНЫЙ ЦЕНТР ПОМОЩИ
ПРОПАВШИМ И ПОСТРАДАВШИМ ДЕТЯМ
НАЙТИРЕБЕНКА.РФ

лига безопасного интернета

Сайт
ligainternet.ru

КАК ОБМАНЫВАЮТ В ИНТЕРНЕТЕ?

Современные мошенники в Интернете действуют не так, как мы обычно привыкли. Сейчас злоумышленники не крадут у нас деньги напрямую. Вместо этого мы сами им их отдаем. Мошенники манипулируют нами, нашей доверчивостью, страхом или жадностью, а современные технические средства позволяют подделать все, в том числе, сайт или номер телефона.

КАКИЕ СХЕМЫ МОШЕННИЧЕСТВА СУЩЕСТВУЮТ?

1. **Взлом аккаунтов в соцсетях и рассылка сообщений от друзей.** Мошенники придумывают разные ситуации и просят срочно перевести деньги.

2. **Сайты-подделки.** Это могут быть копии страниц социальных сетей и Интернет-магазинов. При покупке товара на сайте-поделке ты не получишь ничего, а деньги отправятся напрямую в руки преступников.

3. **Рассылка писем по электронной почте и в соцсетях с выигрышем.** Мошенники вынуждают ввести свои данные для получения выигрыша или отправить им комиссию за получение награды.

4. **Звонки с поддельных номеров.** Мошенники могут представиться кем угодно – работником банка, полиции, госструктуры, врачом, даже твоим родственником.

5. **Шантаж.** Украденные персональные данные или фотографии мошенники могут использовать чтобы вымогать деньги у жертвы. При этом особое внимание преступников направлено на интимные или иные компрометирующие человека фотографии или сведения, которые они крадут, взламывая почту или личную страницу в социальных сетях.

Современные технические средства позволяют мошенникам подделать любой номер телефона, любой сайт, взломать почту или личную страницу. Будьте бдительны и перепроверяйте информацию. Никогда не отправляйте свои интимные фотографии даже хорошо знакомым людям, которым вы доверяете. Знайте, что ваши откровенные фотографии, легкомысленно направленные кому-либо, могут быть украдены, в том числе, для рекламы разного рода неприличных или противоправных услуг. Вы можете узнать об этом только когда ваши близкие или знакомые увидят вас и составят о вас негативное мнение. Впоследствии подобные фотографии также могут быть существенным препятствием для зачисления в ряд ВУЗов или устройства на хорошую работу.

В своей работе мошенники активно используют социальную инженерию. Они сделают все, чтобы ты сам отдал свои деньги. Для этого они используют нашу невнимательность и доверчивость.

Знаешь ли ты, что никому нельзя сообщать свои пароли, пин-коды, коды из СМС и сообщений? В наше время это знают все, но мошенники могут обхитрить неосторожного пользователя. Они позвонят тебе и представятся сотрудником банка, расскажут о том, что прямо сейчас кто-то пытается украсть твои деньги со счета. А чтобы этого не случилось, ты должен сообщить им код из СМС, которая сейчас придет на твой номер. Естественно, никто твои деньги не крал. А вот если ты передашь мошенникам этот код, то они получат полный доступ к твоему счету, карте и всем деньгам, которые на ней лежат.

Мошенники не обязательно запугивают. Они могут сообщить о крупном выигрыше. Допустим, в 300 тысяч рублей. Но чтобы получить этот выигрыш, надо заплатить небольшую комиссию – всего лишь 300 рублей. Многие люди в такой ситуации теряют бдительность и думают, что 300 рублей – маленькая цена за такой большой выигрыш. Однако приз, естественно, они не получают, а лишаются своих денег.

КАК ОБЕЗОПАСИТЬ СЕБЯ ОТ МОШЕННИКОВ?

1. **Настрой в мессенджерах и соцсетях двухфакторную (двухэтапную) аутентификацию.** При попытке входа в свой профиль тебе на почту или в сообщения будет приходить код подтверждения.

2. **Перепроверяй на официальных сайтах номер телефона, с которого тебе позвонили.** Если тебе позвонили, например, из банка или из полиции, представились сотрудником, ты можешь самостоятельно найти в Интернете телефоны этих организаций, перезвонить и спросить у них, действительно ли там работает такой человек, и звонил ли он по твоему номеру и с какой целью.

3. **Проверяй адрес сайта.** Мошенники рассчитывают на невнимательность пользователей и часто делают сайт похожий на оригинал. В адресе сайта может отличаться одна буква или символ.

4. **Обращай внимание на наполнение сайта.** Мошенники часто допускают ошибки в словах и тексте, так как делают сайты-подделки на скорую руку.

5. **Не переходи по незнакомым ссылкам.**

6. **Не открывай файлы из писем или сообщений, которые прислали незнакомые люди.**

7. **Если же ты стал жертвой мошенников, то следует сразу же сообщить об этом родителям.**

ЧТОБЫ НЕ ПОПАСТЬСЯ МОШЕННИКАМ – МЫСЛИ САМОСТОЯТЕЛЬНО!