ЭССЕ НА КОНКУРС «БЕЗОПАСНЫЙ ИНТЕРНЕТ» НА ТЕМУ «ЧТО ДЕЛАТЬ ПРИ ВСТРЕЧЕ С МОШЕННИКАМИ?»

Автор: Додонова Татьяна Константиновна, 9 класс

Образовательное учреждение: Муниципальное бюджетное общеобразовательное учреждение «Дубравская средняя школа»

Адрес ОУ: 606307, Нижегородская область, Дальнеконстантиновский муниципальный округ, сп. Дубрава, ул.Центральная, 13

В наше время, время информации и технологий, всё чаще встречаются мошенники в сети Интернет.

Где же именно они могут вас подстерегать, на каких сайтах и просторах Интернета? Что делать при встрече с ними? Об этом мы сегодня с вами и поговорим.

Каждый человек, взрослый или даже ребёнок встречался с каждым из этих видов мошенников.

Но самым распространённым видом мошенничества является фишинг. Очень схоже с английским словом fishing, которое переводится как «рыбачить». Только в этом случае вылавливают не рыбу, а ваши пин-коды, номера и пароли. Фишинг чаще всего встречается в почтовых отправлениях, социальных сетях, при онлайн-оплате за товары и услуги. Обычно это происходит так: человек получает по электронной почте письмо от определенного сервиса или «знакомой» организации. Причём электронный адрес максимально похож на настоящий, мошенники специально подделывает его. Пользователь переходит по данному адресу, вводит свои данные – и вот, попадается на крючок! В данном случае, чтобы избежать неприятностей, нужно обращать внимание буквально на всё: адрес сайта, текст письма, даже обращение к вам не по имени должно сразу вызвать некие подозрения.

Довольно часто встречаются люди, которые пишут с незнакомых вам номеров якобы от лица ваших родственников. Они просят перевести какую-то сумму на их номер. Хорошо изучив человеческую психологию, мошенники даже могут совершать звонки в неподходящий момент, например, глубокой ночью, когда человек уже давно спит. Они убеждают собеседника в том, что их близкий родственник попал в неприятную ситуацию, и чтобы помочь ему, нужно перевести крупную сумму. Нередко люди верят и даже не узнают голоса своего сына, отца и т.д. Такие сообщения и звонки стоит просто игнорировать и блокировать номер, с которого вам пришло сообщение.

Подвидом таких «телефонных» мошенников можно считать тех, которые звонят вам по номеру, представляясь, например, сотрудником банка. Они просят назвать данные вашей карты, например, под предлогом того, что ваша карта заблокирована или на неё оформлен кредит. В таком случае лучше сбросить трубку и позвонить по горячей линии банка и расспросить их.

В наше время стали набирать популярность такие Интернет-магазины как Wildberris, AliExpress и Авито. Довольно популярные и проверенные сайты, но и их мошенники не обошли стороной.

Конкретно на Интернет-площадке Авито и встречается следующий вид мошенников. «Продавец», заранее завладев чьим-нибудь аккаунтом, предупреждает покупателя, что может отправить товар только по полной предоплате. Получив деньги, он, конечно же, исчезает, не отвечает на звонки и сообщения. Чтобы обезопасить и покупателя, и продавца, данный крупный сайт усиливает меры по предупреждению мошенничества.

Можно ещё встретить побочные, неофициальные сайты, которые запрашивают ваши данные. В таком случае стоит ничего им не предоставлять и внимательно относится к адресам сайтов.

Из-за большого количества атак и попыток взлома аккаунтов пользователей многие сайты используют двухфакторную аутентификацию. Это метод, при котором, прежде чем войти на сайт, пользователю необходимо ввести данные двух разных типов. Он вводит на сайте свой логин и пароль, а затем специальный код, который приходит ему на привязанный к аккаунту телефон или на электронную почту. Это обеспечивает более эффективную защиту от мошенничества.

Заинтересованные в своих пользователях платформы для безопасности предлагают использовать в качестве пароля специально подобранный ключ или усложнить свой пароль путем подбора букв алфавита, цифр и символов.

Мы рассмотрели лишь некоторые виды мошенничества в Интернете. Проанализировав их, можно сделать вывод. Предоставлять свои личные данные, адрес, телефон, номер банковской карты стоит лишь проверенным лицам и Интернет-сайтам, заботящимся о качестве своих услуг и безопасности пользователей. Также стоит проверять подлинность сайтов или номеров, игнорировать звонки и сообщения, поступающие от них.

Конечно, мошенников в сети Интернет очень много, и знать абсолютно все схемы мошенничества невозможно. Но для собственной безопасности достаточно придерживаться общих правил: быть предельно осторожным, не оставлять свои персональные данные на доступных ресурсах, минимизировать «опасные» контакты.