

Опасности в интернете: как не попасться на уловки мошенников?

Преподаватель и ведущий методист кафедры математических основ информатики «Московская школа программистов»

Дмитрий Коняев рассказал об уловках, которыми пользуются мошенники в интернете, использовании социальной инженерии и слабой осведомленности населения о протоколах работы различных служб, а также о том, как без лишних опасений пользоваться интернетом.

Как обезопасить своего ребенка в интернете?

Радикальный метод в виде отключения доступа бесполезен и вреден.

Интернет настолько проник в нашу жизнь, что что-то заблокировать и запретить совершенно невозможно. Поэтому этот вопрос должен лежать в другой сфере — необходимо формировать культуру работы в интернете, и в этом процессе важна роль учителя. В интернете нас могут подстерегать два основных вида угроз:

1. Социальная инженерия.

Социальная инженерия — это метод получения необходимого доступа к информации, основанный на особенностях психологии людей. Например, если человеку надавить на жалость, он может выполнить какое-то действие, которое требует от него мошенник. Другой прием — сказать, что «времени нет», тогда человек станет принимать решение быстро и, скорее всего, допустит ошибку.

2. Вирусы и вредоносные программы, которые могут как уничтожить ваши файлы и операционную систему, так и получить доступ к вашей финансовой информации.

Основные виды мошенничества

Самый популярный вид мошенничества — **взлом аккаунта кого-то из ваших друзей, когда вам пишет человек с просьбой одолжить денег**. Этот вид мошенничества работает, потому что он простой и дешевый. Есть версия, что этим промышляют люди, которые находятся в заключении. *Если вы получаете такое сообщение, то убедитесь, что это реальный человек, спросите у него что-то, что знает только он, либо просто игнорируйте такие сообщения.*

Еще один очень популярный вид жульничества — **это сбор средств**. Здесь как раз в ход идет социальная инженерия. *Вы читаете, и вам с первых строк хочется помочь и дать денег, вам давят на жалость. Для того чтобы не отправлять деньги мошенникам, проверяйте всю информацию: позвоните*

в больницу и узнайте, есть ли у них такой пациент. Семь из десяти объявлений о сборе средств на лечение — фейк.

Кликбейт — заголовок, в котором очень захватывающий сюжет прерывается на самом интересном месте, и нас отсылают читать продолжение в источнике. В большинстве случаев кликбейт относительно безопасен — скорее всего вас просто перенаправит на страницу с рекламными баннерами. Однако такие новости могут быть опасными, потому что туда можно вложить ссылку с опасным контентом.

Еще один вид мошенничества — **выигрыши**. Например, это баннер, картинка или плашка якобы от браузера Google, где заявляется, что ваш IP-адрес был выбран в качестве победителя. Понять, что это мошенничество, очень просто, если хотя бы немного понимать, как работает интернет. Во-первых, собрать базу всех IP-адресов невозможно, а даже если такая база есть, то большинство таких адресов будут серверами, а не личными компьютерами. К тому же, Google никогда не проводит лотереи. Такие розыгрыши — 100 % обман.

Получение чего-либо за низкую сумму, например, телефон за один доллар. После того, как вы перейдете по ссылке, вам предложат, например, оплатить доставку — вы введете свои данные — и в лучшем случае получите нескончаемый поток спама, звонков и рекламы, в худшем — останетесь без денег. Выигрышей подобного рода не существует.

Платные опросы. Опросы действительно стоят денег, и маркетинговые исследования — это всегда довольно затратно. Если компания хочет вывести на рынок новый продукт, то всегда занимается исследованием запросов потребителей. Если вы видите такие предложения, то обратите внимание на предлагаемую сумму, если вам предлагают заработать 25 тысяч рублей за опрос — это обман. На опросах зарабатывать можно, и даже существуют специальные биржи. Однако доход на таких биржах варьируется от 5 до 80 рублей за опрос.

Мошенники на Авито. «Мой друг продавал что-то на Авито, ему покупатель написал, что готов сделать предоплату за товар около 20 тысяч рублей. После этого друг получает звонок из банка: „мы заметили подозрительную транзакцию, она была заблокирована, для разблокировки сообщите код клиента“. Код клиента дает доступ ко всей финансовой информации счета,

и после того как мой друг сообщил код клиента, с его счета сразу была списана крупная сумма денег». *Банки никогда не звонят по поводу безопасности! Банк просто блокирует карту в подозрительных ситуациях.*

Спам. Такие письма почти гарантированно содержат в себе вирус. Спам сейчас — примерно 80 % всего потока писем. Вы получаете такое письмо, переходите по ссылке и дальше идет цепная реакция — одна ссылка перенаправляет на другую (а таких перенаправлений может быть сколько угодно много) и рано или поздно вы получите вирус или требование ввести личные данные.

Документы и файлы. Кажется, что документы безопасны, но это не так. Вирус — это не только исполняемый файл. В документах могут содержаться макросы. Они потенциально очень опасны. Поэтому если вы не пользуетесь макросами, то вам лучше отключить их исполнение в настройках офисных программ.

Как обезопасить себя от угроз?

- Настройте двухэтапную аутентификацию в соцсетях. Это спасет вас в случае компрометации вашего пароля. Двухэтапная аутентификация помогает более надежно защитить ваш аккаунт. Если она включена, для входа используются два компонента: то, что знаете только вы (например, пароль) и то, что есть только у вас (например, телефон или электронный ключ). Установите пароль на учетную запись Windows.
- Создайте отдельную учетную запись для ребенка с отдельным паролем.
- Проверяйте ссылки и файлы. Это можно сделать с помощью VirusTotal.
- Обращайте внимание на замочки в браузере и почте. Если сайт использует защищенный сертификат, то в большинстве случаев ему можно доверять.
- Не открывайте папку спам. Используйте бэкап. Загрузите все свои важные файлы на отдельный диск, который не подключен к интернету. Попробуйте операционную систему Linux. 99 % вирусов написаны для системы Windows.
- Не пытайтесь заработать на подозрительных схемах.
- Мыслите и оценивайте информацию критически.