

OUCH!

Ежемесячник по информационной безопасности

Что знает о тебе Интернет

Обзор

Многие из вас слышали о том, как важно защищать персональные данные онлайн и внимательно следить за информацией, которой вы делитесь в сетях. Чтобы это доказать, мы научим вас искать информацию о себе и узнавать, какая информация о вас есть в публичном доступе. Этот процесс называется OSINT, то есть Данные Открытых Источников (Open Source Intelligence). Это означает поиск в общедоступных интернет источниках с целью получения данных об IP адресе компьютера, компании или человеку, например, о вас. Помните, что злоумышленники используют подобные инструменты и способы для своих целей. Чем больше они соберут информации, тем больше шансов на успех их целевой атаки. Эта концепция существует много лет, но современные инструменты упрощают её практическое использование.

Как искать информацию

Нельзя найти всю информацию на одном сайте. Начать поиск следует на одном сайте, затем используя полученную информацию, приступить к поиску на других сайтах. Затем следует сопоставить и сравнить результаты для составления профайла или досье вашего объекта. Хорошим местом для старта являются поисковые системы, например, Google, Bing или DuckDuckGo. У каждого из этих поисковиков есть различная информация о вас, поэтому вести поиск следует более, чем на одном сайте. Начните с введения имени, заключённого в кавычки в поисковик. Далее следует расширить поиск так называемыми операторами. Операторы – специальные символы или текст, при добавлении которого ваш поиск будет более точным. Это особенно важно, если имя объекта довольно распространённое; вы можете добавить к поиску такую информацию, как адрес электронной почты или город проживания. Получить больше информации об операторах и продвинутых техниках поиска можно в разделе Ресурсы в конце статьи. Примеры поиска:



- «Имя Фамилия» > какую информацию можно получить о человеке
- «Имя Фамилия@» > поиск электронной почты человека
- «Имя Фамилия» filetype:doc > поиск документов Word содержащих имя данного человека

Существуют специальные сайты, собирающие персональные данные. Откройте один из них, и вы узнаете, что доступно общественности о вас. Данные не всегда достоверны и могут быть специфическими для определённых стран. Проверьте информацию путём поиска на нескольких сайтах и сравнения результатов.



- <https://pipl.com>
- <https://cubib.com>
- <https://familytreenow.com>

Есть и другие сайты, на которых можно получить много информации, например, Google Images, Google Maps, всевозможные социальные сети и многие другие. Подробный список таких сайтов можно найти здесь:

<https://osintframework.com>

Зачем искать данные о себе в Интернете?



1. Следует знать, какая информация есть у других людей или организаций о вас, что размещено в сети и чем они поделились. (церковь, школы, спортивный клуб и другие сайты местных объединений).
2. Помните, что вся эта информация доступна каждому, включая злоумышленников, которые могут этим воспользоваться. Будьте бдительны. Следует осторожно относиться к срочным звонкам, например, из банка; не следует доверять звонящим только потому, что у них есть ваши базовые данные. В таких случаях следует вежливо прекратить беседу и самому позвонить в банк по проверенному телефону, чтобы убедиться, что они действительно вам звонили. Такие же действия следует совершать с письмами электронной почты: если к вам обращаются по имени, это совсем не значит, что письмо официальное.
3. Следите за тем, что вы размещаете в сетях, эта информация может навредить вам, вашей семье или работодателю.

Об авторе

Нико Деккенс (@duch_osintguy) занимается сбором данных из открытых источников (OSINT). Он живёт и дышит сбором и анализом кибер данных. Нико читает лекции, посвящённые OSINT, Интернету Вещей (IoT) и Безопасности Рабочих Процедур (Operations Security) для компаний из списка Fortune 500 и правительств многих стран мира.



Ресурсы

Социальная Инженерия:

<https://www.sans.org/u/LW6>

Безопасность в социальных сетях: семь советов:

<https://www.sans.org/u/LWb>

Уточнение поисковых запросов:

<https://support.google.com/websearch/answer/2466433>

OSINT Framework:

<https://osintframework.com/>

Институт SANS Course SEC487: Open-Source Intelligence (OSINT) Gathering and Analysis:

<https://www.sans.org/u/LWZ>

OUCH! выпускается Институтом SANS в рамках программы «Securing The Human». Распространение журнала регулируется **Creative Commons BY-NC-ND 4.0 license**. Вы можете использовать и распространять журнал при условии, что ничего не будете менять. Для перевода или получения более подробной информации, пожалуйста, обращайтесь: www.sans.org/security-awareness/ouch-newsletter. Редакция: Уолт Скривенс, Фил Хоффман, Алэн Вэггонер, Шерил Конли | Русский перевод: Александр Котков, Ирина Коткова