ИНТЕРНЕТ БЕЗОПАСНОСТ

ciela

София • 2016
ISBN: 978-954-28-2174-8

Александър Ненов

ИНТЕРНЕТ **БЕЗОПАСНОСТ**

ciela

СЪДЪРЖАНИЕ

Да се запознаем 11

Как се подслушва цял квартал 13

Обратно на логиката 18

Кредитната и личната карта? 22

Как става хакването на профил? 35

Психологически подход 37

Хигиена на онлайн потреблението 39

Чужди компютри 39

Свободни мрежи 40

Криптирайте всичко 41

Криптирана или текстова парола? 42

Секс услуги на живо от детската стая 46

Какво всъщност се случва? 48

Как става размяната на пари? 49

Що е то виртуална валута? 51

Какъв е рискът при тези услуги? 55

Какво да правим, когато това се случи? 57

Нашите заспаха – ела у дома! 59

Големи пари, малко работа и една хотелска стая 62

Сексуално изнудване 65

Как става изнудването? 65

Как да се предпазим? 68

Приятелите също са проблем 68

Скрита камера 71

Любовни схеми 75

Финансова схема 78

Депресията 79

„Ислямска държава“ 80

Трафик на хора 81

Извършване на престъпление от любов 82

Как да установим, че сме жертва? 82

Внимавайте – бог дебне зад ъгъла 89

Здравните форуми вредят на здравето 92

Агресията е навсякъде 96

Една история, която не трябваше да разказвам… 99

Мотикаря/презареждане 100

Добри практики 103

Бъдете промяната 104

Сигнализирайте! Сигнализирайте! Сигнализирайте! 105

Сигнализиране във Facebook 106

Как работят сигналите? 109

Сигнализиране в Youtube и Vbox7 115

Сигнализиране в порносайтове 116

Програми за родителски контрол 117

Доброволното проследяване 123

Доверието 124

Специални благодарности на моите
консултанти тийнейджъри:
Виолета Дончева, Лора Тенева и Борис Йотов

ДА СЕ ЗАПОЗНАЕМ

В тази книга ще ви разкажа историите на много деца на различна възраст – от 13 до 18 години. Всяка една история е истинска и бъдете сигурни, че няма да ви спестя забавните моменти. Но също така няма да спестя и тези, които ще ви накарат да настръхнете. Защото тези деца не са по-различни от децата отпреди 20 години и можете да сте сигурни, че не са по-различни от вашите собствени.

Средата може да е различна, възпитанието – също, както училището и характерът, но едно нещо важи за всички тийнейджъри независимо от държавата, града или годината на раждане – това е жаждата да правят каквото си искат. Жажда, която може да отведе много младежи по пътя на успеха, а други да тласне към провала.

Преди да говоря каквото и да било, бих искал да ви се представя, но не така, както ме познават хората в интернет обществото. Да, сега съм известен като сериен предприемач, с множество успешни интернет проекти, мениджър, работил във и със някои от най-големите ИТ компании в страната и консултант на най-успешните интернет сайтове у нас. Така ме представят по семинари, лекции и телевизии… Но преди да стана това, което съм сега, съм бил на 13… и, повярвайте ми, тогава бях друг. Е, нека се запознаем

с моето 13-годишно Аз. След като ме опознаете, ще разберете, че написаното от мен в тази книга не са просто думи за безопасния интернет или думи, които някой да ви продаде в лъскава опаковка.

Но нека започнем:

Здравейте,

Казвам се Алекс, на 13 съм и уча биология и химия в ново за мен училище. Първия си компютърен вирус написах[1] в 8-и клас за училищните компютри „Правец 8М“. При стартиране вирусът рецитираше фрагменти от „Ад“ на Данте, след което заплашваше да унищожи компютъра, ако потребителят не въведе правилното продължение на цитата. При грешка мониторът спираше да функционира коректно… Разбира се, бях направил нещата така, че бързо да мога да ги оправя, за да няма истински технически проблеми, които щяха да ми струват разправии с директора на училището, но пък имах немалко проблеми с учителите по информатика.

Защо го правех ли? Защото можех! И защото беше прекрасно всеки да те знае като „хакера“, още повече във времена, когато повечето хора дори не знаеха как се включва компютър.

На 14 (през 1996 г.) за първи път използвах интернет в домашни условия и само няколко месеца по-късно се представях с няколко имена в мрежата като член на организирана хакерска група. Хаквах какво-

[1] Жаргонен израз, описващ програмиране.
(Всички бележки са на автора).

то можех и където можех – по всяко време. На практика всяко електронно устройство представляваше интерес и целта ми беше да получа контрол над него.

На 15 действията ми вече бяха целенасочени – да получа безплатен и неограничен интернет достъп, тъй като тази услуга тогава се таксуваше на час, а родителите ми плащаха само за 5 часа на месец. Представете си колко малко е това, особено погледнато от сегашната реалност, когато всеки има 24-часов достъп до мрежата, и то през няколко устройства. А за да се развивам, аз имах нужда от повече.

КАК СЕ ПОДСЛУШВА ЦЯЛ КВАРТАЛ

За да си осигуря така мечтания интернет достъп, за който да не плащам, но пък и да нямам ограничения, съм правил всевъзможни схеми, като използване на различни телефони и препращачески устройства, за да получа още 1 или 2 часа интернет. Не са били рядкост моментите, когато, за да си осигуря мрежа, съм прехвърлял телефонното обаждане през различни градове на страната и обратно към София с цел да заблудя я централата на БТК, я телефонната централа на доставчика…

Но решението се оказа много по-лесно. Един ден ми попадна програма, която можеше да работи на компютъра, без да се засича от антивирусните програми, но и да не е видима за потребителя. Редактирах я леко и тя стана прекрасен шпионски инструмент, който записва всичко, което потребителят прави на компютъра – всеки клавиш, всяко кликване, всяка

смяна на прозорец… буквално всичко. Не дочаках да правя каквито и да било тестове, а директно посетих най-големия компютърен клуб към момента в София и инсталирах програмата, като я настроих да се включва с компютъра и да записва всичко в едни огромни текстови файлове. За да маскирам файловете, текстът вътре беше кодиран примитивно. Иначе казано, между всяка буква се поставяха произволни символи, които правеха текста нечетим.

Например информацията във файла изглеждаше като безкраен низ от подобни данни. Много хора, дори и да отворят този файл, не биха се ориентирали какво реално има в него:

{k89}П{4t3}о{g34}т{24t}р{er4}е{241}б{v34}и{wby}т{w5y}е{wj6}л{ej5}с{w4y}к{455}о{G35} {rgrw}и{4h3}м{h53}е{j54}:{55h}{wh4}{j4w}s{wj5}u{53h}p{nrw}e{e3t}r{gw4}m{5gw}e{h53}n{yj}П{5w5}a{y42}p{h52}o{hg3}л{5hd}a{ntr}:{ntrw}{he5}u{my8}a{y85}b{tr6}a{r77}d{fh5}u{t5u}b{jty}a

Всяка седмица ходех в клуба, сядах на един от компютрите и през мрежата изтеглях файловете от всички компютри и ги почиствах, за да може другата седмица да има място за новите попълнения. Изпращах файловете по имейл вкъщи, където спокойно си ги изтеглях и разглеждах. За да ги чета обаче, имах нужда от малко съдействие, тъй като виждате – текстът не е особено четим, макар че не бих се изненадал, ако вече сте се досетили как трябва да се стигне до написаното. Нали? Е, аз реших да се улесня, като използвах специална програмка, написана специално за целта (различна от шпионската), за да почисти излишните символи.

Примитивно замаскираният текст по-горе всъщност представлява изречението:

Потребителско име: supermen Парола: uabaduba.

Това може да се прочете, като се премахнат всички символи в къдравите скоби, включително самите къдрави скоби. Да, не е нещо изключително сложно, но целта не беше да се заблуди екип от НАСА или Пентагона, а обикновен служител на компютърен клуб със средна компютърна грамотност. Ето това трябва да научат децата в училище – когато едно нещо може да върши работа по простия начин, няма нужда да го усложняваме излишно, при положение че това не допринася за неговата продуктивност. Е, в случая маскировката работеше прекрасно неограничено време.

След като почиствах файловете, сядах и започвах да чета. Ред по ред, парола по парола.

Имах паролите на целия квартал, а може би и на половината град. Бяха хиляди и нямах идея за какво мога да ги ползвам. Понякога четях пощите на хората ей така, за удоволствие. Имаше потребители, за които знаех повече от собствените им мъже и жени, защото четях кореспонденцията с любовниците им. И така минаваха скучните месеци, докато един ден дойде бленуваната парола. Беше за поща, но не каква да е поща, а от тези, към които има асоцииран Dial-up интернет достъп[2].

[2] Dial-up (дайлъп, или комутируем достъп) – свързване между компютри посредством телефонната мрежа. В ранните годи-

Следващата стъпка беше как, след като имам име и парола, да успея да се свържа с интернет, без да знам телефона за достъп на доставчика, а тогава нямаше и Google. На теория беше сложно, но точно тогава участвах на добра воля (заедно със стотици други хакери) в поддръжката на списък с всички интернет доставчици в страната, техните телефонни номера и централи, IP-та на сървърите, операционни системи, отворени портове… накратко, ако някой искаше да се тества срещу някой доставчик, просто влизаше в каталога, търсеше по име на доставчика и ползваше информацията, която му трябва, за да атакува по начина, който има желание. Разбира се, всеки можеше да се снабди и сам с тази информация, но това отнемаше време, а каталогът наистина беше доста богат. Да намеря телефона за достъп до доставчика бе най-лесното нещо от процедурата и няколко минути по-късно имах неограничен интернет достъп. Ползвах този акаунт в продължение на година и половина, а родителите ми така и не разбраха, че платените от тях 5 часа на месец са се превърнали в неограничен интернет достъп за без пари.

През тези славни за моето тийнейджърство години аз се научих да програмирам на редица програмни езици, да взимам контрол над всякакви машини, да „подслушвам“ чатовете на моите приятели, познати и непознати, да провеждам безплатни разговори с България и по света от чужди номера, дори със

ни на интернет това беше основен начин за осъществяване на връзка между потребителите и интернет доставчиците.

способ, който и телефонните централи не можеха да разберат. На практика бях свикнал да боравя с техниката по начин, който ми гарантираше внимание в училище и във всяка компания и усещането, че мога и правя нещо, което другите само могат да мечтаят… или дори нямат идея как да мечтаят за това, защото им е напълно непонятно… Стигал съм до степен да си играя с апарати като телекс[3] – нещо, което в момента младите дори не знаят какво е, но посредством това подобно на компютър устройство успях да се свързвам с различни пощенски станции из страната, докато стоях във фирмата на майка ми да я чакам…

Сега, 20 години по-късно, пиша тази книга, защото основните неща не са се променили много и те отново ни застрашават. Но ако преди 20 години аз бях тийнейджър и се забавлявах с невинни щуротии, а интернет беше нещо сравнително непознато и хората бяха мнителни към него, сега нещата са по-различни. Сега и аз съм различен, защото ежедневно ми се налага да се боря с хакерски атаки, опити за измама по всевъзможни начини, софтуерни продукти, имащи за цел да направят уязвим компютъра или уебсайтовете ми, и… разбира се, тийнейджъри, които имат безкрайно много свободно време и завидна техника, с помощта на която биха искали да пробват уменията си срещу някого.

Защо го правят ли? Защото могат!

---

[3] Телекс е вид телеграфен апарат, съставен от телетип и телефонен апарат с шайба за набиране на номера, използвана за предаване на текстови съобщения по прост електрически канал.

Но към тази не съвсем основателна причина има и други мотиви, които карат един или друг човек да извършва конкретни зловредни, опасни или престъпни действия в мрежата. Новите технологии дадоха възможност да се извършват дейности, за които повечето хора дори и не предполагат. Е, време е да започваме с кошмарите.

ОБРАТНО НА ЛОГИКАТА

Повечето наръчници за безопасен интернет съветват хората да не дават личните си данни в мрежата. По възможност те винаги трябва да са измислени, фалшиви, за да се запази абсолютна анонимност. Това беше валидно за онези далечни времена, когато интернет прохождаше. Сега анонимността може да ви нанесе много повече вреди, отколкото можете да си представите.

Един от съветите ми към всички мои познати и приятели винаги е бил: Давайте номера на телефона си свободно на Google, Facebook, Microsoft, PayPal или други подобни компании, стопанисващи някои от най-големите сайтове в света. Причината за съмнението у потребителите е, че те очакват профилът им в тези мрежи да бъде хакнат или по един или друг начин личният им телефон да стане обществено достояние. Същото е и с адреса, датата на раждане и дори името. Липсата на тези данни в профила ви рядко успява да спре или затрудни наистина заинтересованите лица да хакнат профила ви, но може да се окаже голям проблем в случай на атака срещу вас.