Тимощук Богдан Анатолійович
2 курс, факультет соціології і права,
НТУУ «КПІ»
Науковий керівник:
Бежевець А.М., старший викладач
кафедри інформаційного права та права
інтелектуальної власності ФСП НТУУ «КПІ»

Кібер-злочини: різновиди та способи застереження

На мою думку, кібер-злочини - найбільш актуальна та найбільш небезпечна сфера злочинів. Оскільки наука та техніка не стоїть на місці, з'являються злочинці, які цим користуються. «Зеленим світлом» для хакерів став розвиток мережі інтернет, її поширення майже у всіх країнах світу. Мабуть кожен задасться питанням: що саме потрібно хакерам щоб обманути користувача мережі? Невже, просто наявність комп'ютера? Звичайно, не тільки. Якщо компьютер не підключений до мережі інтернет, то ви не цікаві сучасним злочинцям. Але людина - активний користувач мережі інтернет, соціальних мереж, або хоч декілька разів завантажувала програми - може бути в так званій зоні ризику.

Зокрема, якщо персональні дані потраплять до рук зловмисників - вважайте себе ошуканим. Номер телефону, сторінка в соціальних мережах, домашня адреса, серія та номер паспорта, ідентифікаційний код – будь-яка з переліченої інформації потрапить до зловмисників – і вони зможуть віднайти решту. А якщо вони віднайдуть все інше, то пограбувати, ошукати, або просто зіграти з людиною злий жарт стане простіше простого.

На даний час не обов'язково бути хакером, щоб маючи номер телефону, дізнатися про людину все, від домашньої адреси до номеру банківської картки, номеру автомобіля, місця перебування та, навіть, копії паспорта. Ця інформація коштує від 15 до 30 доларів в залежності від обсягу та складності пошуку. Зазвичай такими послугами користуються в благих цілях - розшукати боржника або віднайти власника автомобіля, який завдав шкоди і зник з місця ДТП.

Кваліфікованому хакеру віднайти персональні дані не складе великих зусиль.

Достатньо увійти в одну з потрібних баз. Найбільш небезпечними випадками є вторгнення хакерів у бази даних банків, коли до їх рук потрапляють номери рахунків. Розумні шахраї будуть декілька разів через деякий час знімати з рахунку по 1-2 гривні. Це та сума, нестачу якої важко помітити, а якщо людина і помічає, - то не рахує це великою втратою, та не хоче марнувати свій час на сварки з банком. Однак, якщо підрахувати кількість клієнтів, наприклад, Приватбанку (на 2015 рік більш ніж 20 мільйонів осіб) і помножити на 1-2 гривні, то можна порахувати, яку суму шахраї знімуть за один раз без особливих підозр.

Шахрайство хакерів не зупиняється на розголошенні персональних даних третім особам та обкрадання банківських рахунків. Найбільшу небезпеку становлять кібер-злочинці, які працюють у сфері взлому військових серверів, військових таємниць та військових потужностей держави. Історія знає безліч випадків взлому та викрадення таємних розробок НАСА, НАТО, не говорячи про можливість потрапляння інормації про засекречені військові бази однієї країни до іншої. Такі «генії» загрожують існуванню не однієї чи кількох осіб, а цілим країнам, а навіть континентам.

Хакери поділяються на «чорних» та «білих». Про чорних я розказано вище, а про білих мова йтиме далі. Це особи, які використовують свої знання та вміння на користь держави, компанії, на яку вони працюють, та ін. Вони не взламують, а, навпаки, захищають бази даних, або ж повертають їх у законне користування власникам.

Єдиним засобом застереження від кібер-шахрайства є захист своїх персональних даних. Необхідно ретельно перевіряти надійність установ, яким ви довіряєте свої дані, а також умови, на яких ви погоджуєтеся на передачу своїх персональних даних.