УДК 343.985.5

ЦИПАК ІЛЛЯ ГЕННАДІЙОВИЧ

курсант групи Ф-4-301 факультету № 4

Харківського національного університету внутрішніх справ

ОНИЩЕНКО ЮРІЙ МИКОЛАЙОВИЧ

кандидат наук з державного управління, доцент,

доцент кафедри кібербезпеки та DATA-технологій факультету № 6

Харківського національного університету внутрішніх справ

СМІШИНГ ЯК ВИД ШАХРАЙСТВА У КІБЕРПРОСТОРІ

Шахраї не стоять на місці, і відколи у людей з'явилися мобільні телефони, вони майже миттєво почали вигадувати нові види обману. Вони дзвонять людям з метою виманити гроші, відправляють смс та займаються спамом. Пропонується розглянути такий вид шахрайства, як смішинг. Смішинг є телефонним шахрайством за допомогою смс повідомлень, який спрямований на недосвідчених користувачів та літню частину населення.

Смішинг – вид фішингу через смс повідомлення, який походить від слова "смс", тобто Smishing. Він не обов'язково реалізується через смс-повідомлення на телефон, а й проводиться за допомогою месенджерів, електронної пошти тощо. Смішинг-атаки зазвичай запрошують користувача перейти за посиланням, зателефонувати за номером або зв'язатися за електронною адресою, наданою зловмисником у повідомленні. Далі жертві пропонується надати свої приватні дані; часто це можуть бути дані інших сайтів або служб. Крім того, через природу мобільних браузерів, URL-адреси можуть відображатися не повністю; це може ускладнити ідентифікацію підробленої сторінки входу в систему. Оскільки ринок мобільних телефонів насичений смартфонами, які мають швидке підключення до інтернету, шкідливі посилання, надіслані в SMS, можуть мати той же результат, що й при надсиланні електронною поштою. Смішингові повідомлення можуть надходити з телефонних номерів у дивному або незрозумілому форматі.

Смішинг може бути як звичайним виманюванням грошей пересічних громадян через смс-повідомлення, так і виманюванням грошей у юридичних осіб, використовуючи людський фактор співробітників компаній, підприємств, установ, організацій тощо. Все залежить від навичок шахрая ввести в оману потенційну жертву.

Смішинг є шахрайством пов'язаним із соціальною інженерією, тобто для отримання своєї цілі шахрай не використовує спеціальні програми або навички хакінгу. Для цього зловмиснику лише потрібні навички спілкування та аналізу поведінки людей. Не виключено, що шахраєм може бути дипломований психолог, який знає людську натуру на найвищому рівні.

Методи соціальної інженерії дозволяють зловмисникам маніпулювати жертвою під час прийняття рішень. Якщо розглядати основні способи реалізації шахрайської схеми, то можна визначити такі критерії:

- **довіра**: шахраї можуть бути дуже розумні в сфері соціальної інженерії, можуть втертися в довіру настільки добре, що жертва відчуватимете в ньому споріднену душу і в змозі зовсім забути про кібербезпеку в мережі Інтернет;
- **контекст повідомлення**: шахраї використовують обставини та інформацію, яку вони дізналися з життя жертви, проти неї або розсилають спам про подію, що трапилася з близькою людиною жертви, наприклад аварія, травма, інцидент з поліцією тощо;
- **емоції**: посилюючи емоції жертви шляхом створення психологічного тиску, зловмисники можуть перекрити її критичне мислення та спонукати до швидких дій, моделюючи ситуацію, де нема часу на обміркування та неквапливе прийняття рішення.

Як захистити себе від Смішингу? Насамперед, це залежить від здатності цільового користувача ідентифікувати смішинг-атаку та проігнорувати повідомлення або повідомити про нього. Захист від смішинг-атак може здійснювати стороння особа/установа, наприклад, надсилаючи клієнту

повідомлення у вигляді попередження від оператора мобільного зв’язку, банку тощо.

У шахрайських смс-повідомленнях можуть бути запити надіслати дані банківської карти. Ніколи не слід робити це, адже у будь-якого банку такі дані зберігаються у надійно захищеній базі даних. Шахрайські смс-повідомлення можуть містити пропозиції швидко забрати великий виграш із посиланням унизу, що звичайно ж веде на сайт шахрая, або на завантажувач шкідливої програми, що може зчитувати особисті дані жертви. Не варто залишати в телефоні, у нотатках або іншому додатку свої особисті дані або дані свого банківського рахунку.

Чи можна зробити так, щоб ці повідомлення не потрапляли на телефон? На жаль, важко запобігти тому, щоб смішінг-повідомлення потрапляли на телефон. Відкритий характер обміну SMS-повідомленнями означає, що кожен може надіслати SMS на будь-який номер телефону. Єдине що може захистити користувача – це його розсудливість, обережність та відсутність панічних настроїв у нестандартних та критичних ситуаціях.

Не розповсюджуйте дані або номер телефону. Зазвичай номери телефонів потенційних жертв смішингу беруться з незахищених баз даних, які можуть зберігатися на сайтах купівлі/продажу або в опублікованих оголошеннях, зокрема комерційного характеру. Витрати часу на роздуми про автентичність потенційно небезпечного текстового повідомлення (надто привабливого змісту або навпаки такого, що вимагає швидкого прийняття рішення та дій щодо надання певної інформації) значно допоможе запобігти успішній атаці смішингу.

Отже, смішинг не є страшною та ефективною хакерською атакою. Це доволі примітивна шахрайська схема, розрахована на неуважних людей, і на неї важко потрапити, якщо витрачати більше часу на осмислення тексту повідомлення.

UDC 351.74:005.591.6