[정보보호] Click fraud, 클릭 한 번도 주의하세요.

스마트 자동차, 스마트 도시, 사물 인터넷 등은 요즈음 우리가 흔하게 접할 수 있는 IT 관련 용어들이다. 어느덧 우리 주변에는 수 많은 IT 관련 기기나 서비스가 제공되어지고 있고 특정 분야와 관계가 없는 사람들조차도 IT라는 말은 전혀 낯선 말이 아니며 SNS나 인터넷의 무분별한 사용으로 자신의 개인 정보가 자의가 아니게 새어나가는 시대가 되었다. 그러나 상당수의 많은 사람들은 이러한 해킹이 영화에서나 볼 수 있고 나와는 상관없는 일이 아닌가 하는 생각을 하고 있는 듯하다. 실제로 해킹으로 인해 나의 소중한 정보가 새어나가고 혹시라도 나의 은행 계좌에서 돈이라도 없어진다면 그 중요성을 피부로 인식할 수 있을까? 모든 것이 온라인으로 가능한 세상에 사는 우리들은 항상 해킹이라는 위협에 노출되어 있음을 인식하는 것이 중요하다. 자신의 정보는 자신이 지킨다는 기본 방어 개념이 갖추어진다면 해킹 시도는 훨씬 어려운 국면을 맞이할 것이다.

그런데 다른 관점으로 우리 주변의 일상을 살펴보면 해킹이 반드시 나와 상관없는 큰 일이 아닐 수도 있다는 것을 깨닫게 된다. 해킹이라는 말을 용어 그대로 해석하면 그럴지 모르지만 좀 더 광범위하게 고려하면 나의 정보나 재산이 나의 의지와 반해 타인에게 넘어가는 현상도 생각해볼 수 있는 것이다. 다양한 전자기기의 발달로 우리는 원하는 정보를 손쉽게 찾아 이를 효율적으로 활용하는 시대에 살고 있다. 그러나 이러한 시대에 살고 있는 우리는 정보의 손쉬운 획득 못지 않게 정보의 유출로 인한 피해를 보기도 하는데 그것이 바로 주변에서 자주 들을 수 있는 스팸이니 해킹이니 보이스 피싱이니 하는 것들이다. 이러한 점은 정보화와 스마트 기기의 발전에 대한 이로운 점을 생각하는 것을 넘어 빈번해진 발생으로 인해 사회 문제화되고 있는 실정이다.

본 고에서는 인터넷 광고나 이메일의 첨부로 보내지는 광고, 전화로 인한 사기, 문자 메시지를 통한 사기 등에 사용자가 슬기롭게 대처하고 자신의 피해를 최소화할 수 있는 방법에 대해 기술하고자 한다. Click fraud란 인터넷에서 광고 링크에 대한 관심이 없는 사용자가 한 번의 잘못된 클릭을 통해 클릭에 대한 대가를 치루도록 만드는 것과 같은 일종의 사기 수법이다. 이러한 click fraud의 종류에는 다음과 같은 것들이 있다.

1) 보이스 피싱: 전화로 수사 기관, 정부 기관, 금융 기관 등을 사칭해 돈을 송금하게 하거나 개인 정보, 금융 정보 등을 물어보는 사기 수법

2) 문자 스미싱: 악성 앱 주소가 포함된 휴대폰 문자(SMS)를 대량으로 전송 후 이용자가 악성 앱을 설치하도록 유도하여 금융정보 등을 탈취하는 사기 수법

3) 파밍: 이용자 PC를 악성코드에 감염시켜 정상 사이트로 접속해도 이용자 모르게 가짜 사이트로 유도하여 금융정보 등을 탈취해 가는 사기 수법

이러한 다양한 사기 수법에 대한 기본적인 대처 요령은 다음과 같다.

- 개인정보 노출을 최소화 시켜야 한다.

보이스 피싱이나 스미싱 등은 개인정보가 누출 되었을 때 발생될 위험성이 매우 커지므로, 인터넷과 같은 공개된 장소에 개인정보 노출을 최소화 하여야 한다.

- 휴대폰 문자에 포함된 인터넷 주소 클릭을 주의하여야 한다.

스미싱의 경우, 노출된 개인정보 등을 이용하여 악성코드가 포함된 인터넷 주소를 송신하는 경우가 많으므로 휴대폰 문자에 포함된 인터넷 주소의 클릭은 매우 높은 경각심을 가지고 있어야 한다.

- 휴대폰을 안전하게 관리하여야 한다.
  - 스마트폰의 권한을 임의로 변경하지 않도록 한다.
  - '알 수 없는 출처(미인증) 앱 설치'에 매우 유의하여야 한다.
  - 스미싱 차단 앱을 설치 하는 것도 한 방법이다.
  - 모바일 백신 앱을 설치한다.
  - 스마트폰의 운영체제를 최신 버전으로 항상 업데이트 한다.
  - 보호되지 않은 무선 공유기(WiFi) 사용을 자제하며, 사용시 많은 주의를 기울인다.

- PC 악성코드 감염에 유의하여야 한다.

파밍 사이트에 연결되는 주요 원인은 사용하는 PC가 악성코드에 감염되었기 때문이며, 이 경우 인터넷 주소창에 정상 주소를 입력하더라도 파밍 사이트로 연결되게 된다. 따라서, PC에 악성코드가 감염되지 않도록 주의하여야 한다. 예를 들어, 컴퓨터 백신 프로그램 (anti-virus program)을 최신 상태로 유지하고, PC의 보안점검을 주기적으로 실시하며, 운영체제 혹은 주요 응용프로그램의 보안 업데이트를 주기적으로 실행한다.

이러한 내용을 담은 기고문이 2017년 3월에 열린 제28차 ASTAP forum에서 가이드라인 형태로 기고되었고 이를 반영한 가이드라인인 'Guidelines for secure use of IT devices and services – Security: Protect your data –'가 회의에서 최종 승인되어 아태 지역 회원국들 간의 정보 공유와 회원국의 일반 사용자들을 위해 공표되었다. 이 가이드라인은 3년여에 걸쳐 개발되어 다양한 상황에서의 사용자를 위한 정보를 제공하고 있다. 이러한 가이드라인의 보급을 통해 우리나라의 사용자들도 안전하게 IT 관련 기기나 서비스를 사용할 수 있기를 기대해본다.

류희수 (경인교육대학교 수학교육과 교수, hsryu@ginue.ac.kr)