[정보보호] 스마트폰에서의 금융 거래, 과연 안전한가?

예전에 우리는 정해진 시간에 은행에 가서 예금을 하거나 필요한 만큼의 돈을 찾는 거래를 행한 적이 있다. 그 당시에는 요새 누구나 들어본 적이 있는 주식이나 펀드 등은 들어본 적도 없으며 주로 예금이나 적금의 업무가 은행 창구에서 이루어지곤 하였다. 그 업무의 대부분도 돈을 입금하거나 인출하는 것이 대부분이었고 가끔 남에게 돈을 전달하기 위해서는 지금처럼 간단하게 이체가 이루어지지 않고 현재 외국에 돈을 보내는 것과 같이 복잡한 단계를 거쳐 이루어지기도 하였다. 시간이 지나고 통신기기의 발달로 이러한 불편함은 간단하고 편리한 방향으로 개선되었고 예전의 주요 업무였던 예금 입출금은 요즈음은 기계가 대신하고 있다. 어느 순간엔가 나타난 전화를 이용한 텔레뱅킹은 우리가 직접 은행에 가지 않고도 은행 관련 업무를 볼 수 있다는 접근성과 용이성을 우리에게 가져다 주었으며 컴퓨터와 통신기기의 갑작스런 발달로 드디어 인터넷을 이용하는 전자금융 시스템이 우리 생활에 깊이 뿌리내려 사용되고 있는 실정이다. 휴대폰이 3세대로 넘어오면서 언제 어디서나 가능한 유비쿼터스라는 개념이 실용화되기 시작하고 실제로 요새는 스마트폰의 도입과 급속한 전파로 인해 휴대용 단말에서의 전자금융 업무는 기하급수적으로 늘어나게 되었다. 실제로 대부분의 스마트폰 사용자들은 자신의 스마트폰에 공인인증서를 내려받아 이를 이용하여 금융 거래와 인터넷 쇼핑을 즐기며 편리한 생활을 영위하고 있다. 그러나 이러한 편리성의 이면에는 우리가 요즘 신문지상이나 매체에서 자주 접하게 되는 해킹이나 피싱, 스미싱 등의 전자적 공격에 취약함이 존재하고 있다. 열 명의 경찰이 한 명의 도둑을 막을 수 없다는 말에서도 알 수 있듯이 사이버 수사대나 통신 사업자의 노력만으로는 이러한 문제를 다 해결하기 어려운 일이며 최종 사용자들의 각별한 관심과 주의만이 이러한 불법 공격의 피해를 최소화할 수 있는 방안일 것이다.

요새 수시로 어느 기관의 중앙 서버가 다운되고 해킹을 당했으며 어느 포털 사이트의 경우 개인 정보가 모두 유출되어 심각한 문제라는 등의 기사나 뉴스가 자주 우리 귀를 어지럽히고 있다. 이러한 현상은 인터넷을 통한 공격 기술의 발달과 개인 정보보호에 대한 부주의한 의식 때문에 점점 더 문제가 될 가능성이 있다. 이러한 일들이 실제 우리의 금융 거래에까지 발생한다면 금전적인 손해뿐만 아니라 사회의 여러 가지 시스템이 불통되는 사태까지 이를 수도 있을 것이다. 이는 현대 스마트 정보화 시대에 크나큰 재앙이 아닐 수 없다.

2012년 12월의 통계 자료에 의하면, 전세계 스마트폰 사용자 수는 11억 명을 넘어서는 것으로 나타났으며 이 수치는 1년 가까이 지난 지금 훨씬 더 많은 사용자를 끌어들였을 것이다. 과거 휴대폰은 음성 수단이었던 반면, 현재의 스마트폰은 다양한 사회·문화적 편익을 주는 하나의 '생활 플랫폼'이다.

그러나, 이러한 스마트폰의 급격한 확산은 여러 가지 삶의 질을 향상시킬 수 있게 한 반면에, 정보보호 문제로 인한 피해사례도 급증하고 있는 상황이다. 이처럼 스마트폰의 활용성은 매우 높은 편의성을 제공하고 있으나, 이를 악성코드 등으로부터 지키기 위한 사용자 개개인의 적극적인 노력이 필요한 시점이다.

따라서, 이러한 상황에 대처하기 위해서는 전자금융을 사용하는 이용자들이 아래와 같은 예방법을 준수하는 것이 매우 유용할 것이며, 이러한 내용들은 뒤에 언급할 국제 표준화 회의에서도 논의가 활발히 이루어지고 있다.

인터넷뱅킹을 안전하게 이용하기 위해서는 각종 비밀번호를 분실·추측·노출되지 않도록 자주 변경하여야 하며, 비밀번호를 잊어버리지 않도록 자신만의 특정한 규칙을 만들어서 관리하는 것이 안전하다. 또한 분실·도난 및 복제의 가능성이 있는 인증수단은 항상 신분증과 같이 몸에 지니고 다니는 등 관리를 철저히 해야 한다.

일반적으로 사용자 관점에서 안전한 전자금융거래를 위한 주의사항을 아래와 같다.

- 거래하고 있는 은행에서 제공하는 보안 프로그램은 반드시 설치하도록 한다.
- 전자금융에 필요한 정보는 PC, 수첩, 지갑 등 타인에게 쉽게 노출될 수 있는 매체에 저장 또는 기록하지 않고 금융회사 직원을 포함한 누구에게도 알려주지 말아야 한다.
- 금융계좌 등의 각종 비밀번호는 서로 다르게 설정하고 주기적으로 변경해 주어야 한다.
- 전자금융거래 이용내역을 본인에게 즉시 알려주는 휴대폰 서비스 등을 적극 이용하라.
- 금융거래 사이트는 주소창에서 직접 입력하거나 즐겨찾기로 사용하고 접속 후 잔액을 조회하여 피싱사이트에 속지 않도록 한다.
- 다수의 일반 대중이 이용하는 공용 장소에서는 인터넷 금융거래를 자제하여야 한다.
- 바이러스백신, 스파이웨어 제거프로그램을 이용하고 최신윈도우 보안패치를 적용하여야 한다.
- 의심되는 이메일이나 게시판의 글은 열어 보지 말고, 첨부파일은 열람 또는 설치하기 전에 백신 등으로 먼저 검사하여야 한다.
- 대출을 이유로 선입금, 잔고 유지를 요구하는 경우 또는 상식수준 이상의 파격적인 대출조건을 제시하는 경우 먼저 사기로 의심하고 거래하는 금융회사의 콜센터 등에 직접 연락하여 확인하여야 한다.

지난 2012년 8월에 개최된 제20차 ASTAP Forum 회의에서 정보보호 전문가 그룹(EG IS)은 정보보호관련 유용한 정보를 제공할 수 있는 정보보호 핸드북(Security handbook)을 작성하기로 동의하였다. 그 후속 작업으로 한국에서는 2013년 3월에 태국 방콕에서 개최된 제21차 ASTAP Forum 회의에 정보보호 핸드북 작성을 위한 목차를 제안하였으며 회의에서는 이를 반영하여 차기 회의부터 정보보호 핸드북 작성의 세부 주제를 정하고 이에 대한 작업을 진행해 나가기로 결정하였다.
또한 제21차 회의에는 한국에서 스마트폰 보안 고려사항에 대한 기고문도 제안되었고 이에 대한 보완 작업이 올 9월에 열렸던 제22차 회의에서 이루어져 최종 수정본을 제23차 회의에서 채택하기로 결정하였다. 이와 함께 제22차 회의에서는 안전한 전자금융거래를 하기 위해

사용자가 주의해야 할 사항들이 제안되었고, 향후 이를 기반으로 전자금융거래를 안전하게 하기 위한 사용자 측면의 주의 사항들을 추가 수정하기로 결정하였다. ASTAP forum의 정보보호 전문가 그룹에서 작성 중인 정보보호 핸드북은 일반 사용자들을 위해 작성되고 있으며 정보보호의 주제별로 매 회의마다 새로운 주제가 제안되고 이에 대한 문서 작업이 이루어지고 있다. 정보보호 전문가 그룹은 핸드북에 대한 작업을 2015년 완료를 목표로 전문가들의 참여와 의견 반영을 통해 만들어가고 있다. 정보보호 핸드북 작성은 지난 3-4년간 아태 지역 정보보호 전문가들의 관심사였으며 이에 대한 준비 작업으로 아시아태평양전기통신협의체(APT) 회원국들 전문가들의 설문 조사를 통해 이러한 문서의 필요성을 인식하고 ASTAP Forum에서 이에 대한 준비 작업을 시작하였다. 이번 회의에서 결정된 사항으로는 개발되는 문서들을 핸드북 형태로 만들지 아니면 권고안(recommendation) 형태로 만들지에 대해 추후 논의하기로 하였으며 핸드북에 대한 목차를 차기 회의에서 최종 결정하여 문서 형식에 따라 모든 문서를 동일하게 작성하기로 하였다.

인터넷과 스마트폰의 사용은 다양한 활용성과 함께 편리한 기능으로 단시간에 우리의 생활 속에 깊이 파고들었지만 이제는 우리는 그 편리함에만 안주할 것이 아니라 그것이 가져다 줄지도 모르는 위험에 항상 대비하여야 한다. 아무리 시스템이 잘 갖추어져 운영되고 있더라도 사용자 개개인의 안전 불감증은 편리함을 넘어서는 더 큰 재앙을 우리에게 가져다 줄 수 있다는 점을 항상 명심하고 이에 대해 대비해야 할 것이며 본 고에서 제시한 방법들이 전자금융거래에서 여러분의 피해를 줄일 수 있는 방안이 되기를 희망한다.

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