사이버안전 (Cybersecurity)이란 무엇인가?

Joshua I. James[1]

2013년 3월 25일

지난주 한국의 몇몇 기관들이 사이버공격을 받았다. 이를 계기로 한국에서는 사이버안전에 관한 논의가 촉발되었고, 이 이슈를 지켜보면서 나는 한국이 '사이버안전 (Cybersecurity)'을 어떻게 이해해야 하는지 어려움을 겪고 있다는 점을 알게 되었다.

여러 논의를 검토한 결과, 여러 기관을 대표하는 사람들이 안전이라는 개념을 경찰이나 군과 같은 조직의 개념으로 이해하고 있는 것으로 나타났다. 그러나 사이버안전은 조직이나 기구가 아니다. 이는 단일한 그룹에 의해 보장될 수 있는 것이 아니다. 사이버안전은 기술을 사용하는 사람이라면 누구나 가지고 있어야 할 책임, 즉 일종의 사고방식이다. 한국의 사이버안전을 지키는 데 있어 모든 사람이 자신의 역할을 하는 것이 필요하며, 자신이 사용하는 기기의 보안을 유지하는 데 주의를 기울이지 않는 사람은 자신뿐만 아니라 자신의 친구, 가족, 직장, 은행, 정부 등 모두에게 위험을 주게 된다.

물론 기존의 조직이나 기관이 사이버안전의 제고에 일정 부분 기여를 할 수 있다. 예를 들면 사이버범죄에 대한 수사를 통해 경찰은 사이버범죄자들을 검거함으로써 잠재적으로 온라인 범죄를 줄일 수 있다. 그러나 경찰이 모든 사건을 해결할 수 없을 뿐만 아니라 조직 성격상 대응적인 성격을 가질 수밖에 없다. 시민들이 사이버안전을 위한 정부의 지나친 개입 (예를 들면 사전적인 모니터링을 통해 '바람직하지 않은' 링크에 접속하지 못하도록 하는 조치) 을 원하지 않는 한, 한 국가의 사이버안전은 모든 사람에 대한 교육을 통해 달성되어야 하는 것이다.

모든 시민과 기업, 그리고 정부기관에서 인식해야 할 사실은 바로 자신이 사용하는 전자 기기가 사이버공격으로부터 결코 자유롭지 못하다는 것이다. 안전을 시간의 개념으로 생각해보라. 가장 강력한 보안조치일지라도 시간만 충분히 주어진다면 얼마든지 무력화될 수 있다. 그러므로 사이버공격을 예방하려면 해커들이 보안조치를 공략할 시간을 주지 않는 것이 가장 효과적이다. 비밀번호를 자주 변경하고, 자신이 사용하는 휴대전화와 컴퓨터를 매 6개월에서 12개월마다 다시 포맷하라. 소프트웨어의 업데이트가 제대로 되었는지를 점검하고, 자신이 사용하는 모든 장비에 안티바이러스와 방어벽을 사용하고, 특히 자신이 사용하는 소프트웨어와 접속하는 웹사이트를 신중하게 골라야 할 것이다. 온라인 안전에 대한 정보는 널려 있고[2], 이 중 가장 기본적인 것만이라도 이해하고 적용하는 것이 사이버안전을 위한 첫걸음이 된다. 시간이 그리 많이 들지도 않지만, 이 작은 실천을 통해 자신과 자신이 사랑하는 사람을 보호할 수 있을 뿐만 아니라 안전조치를 취하지 않아 사후에 겪게 될지도 모르는 불편을 덜어줄 수 있다.

---

[1] 아일랜드 더블린대학교 (University College Dublin) 디지털 포렌직 수사 연구 그룹 (DigitalFIRE: Digital Forensic Investigation Research Group)

[2] 예를 들어 구글에서는 사이버안전 요령을 다음 웹사이트에서 제시하고 있다: www.google.com/intl/ko/goodtoknow 이외에도 www.kisa.or.kr 이나 www.ctrc.go.kr 을 참조하라.

사이버범죄는 매우 역동적이라는 점을 기억하자. 어제 효과가 있었던 안전조치가 오늘은 제대로 작동하지 않을 수도 있는 것이다. 따라서 우리는 전자기기에 대한 안전조치를 취하는 것을 일시적인 노력으로 생각하지 말고, 몸에 밴 습관처럼 일상화해야 한다.