개인의 디지털 보안을 위한 10가지 팁

마지막 업데이트 : 2017년 12월

시작하기에 앞서 가장 먼저 기억해야 할 점은 항상, 100% 안전한 것은 존재하지 않는다는 것입니다. 보안이란 팀 스포츠 처럼 조직, 커뮤니티, 네트워크 내에서 이루어지는 공동의 노력이나 다름 없습니다. 또한 기술은 끊임없이 변화하고, 새로운 취약점은 날마다 발견되며, 위협들은 끊임없이 진화하고 있기 때문에 디지털 보안은 특별히 더 어려운 문제로 다가옵니다. 하지만, 모든 사람들이 비교적 쉽게 실행할 수 있고 이로써 보안상태를 즉시 기하급수적으로 향상시킬수 있는 방법들 또한 존재합니다. ***개인의 디지털 보안을 위한 10가지 팁***은 바로 이 부분을 충족시키고 당장 당신과 당신의 조직이 수행할 수 있는 것들에 대한 개요를 제공하기 위해 작성되었습니다.

1) 소프트웨어들을 최신 상태로 유지하십시오. 소프트웨어들의 업데이트들은 대부분 당신을 악위적인 공격자로부터 취약한 상태로 남겨둘 수 있는 보안문제 또는 버그를 제거하기 위해 개발되고 배포됩니다. 업데이트가 배포되는 즉시 적용하는 것을 권장합니다.

2) 강력한 비밀번호를 사용하십시오. 모든 서비스와 기기들에 동일한 비밀번호를 사용하지 마십시오. 또한 KeePassXC (https://keepassxc.org/) 와 같은 비밀번호 관리 프로그램을 이용하면 각종 서비스 및 기기들을 위해 각각 다르게 생성되는 강력한 비밀번호들을 하나하나 기억하지 않고도 사용할 수 있기에 권장합니다.

3) 해당 링크를 클릭하지 마십시오! 알수없는 출처나 다른사람을 사칭한 출처로부터 전송된 악의적인 링크들이 바로 사람들이 해킹당하는 가장 일반적인 방법입니다. 만약 수상한 링크를 목격하게 되면 클릭하지 않는 것을 권장합니다. 발신자와 링크주소를 주의 깊게 확인하시기 바랍니다. 또한 https://www.virustotal.com/#/home/url 과 같은 곳에 수상한 링크를 조심히 복사 및 붙여넣기하여 이미 악의적인 링크로 신고되었는지 확인해볼 수도 있습니다.

4) 그 첨부파일을 열지 마십시오! 링크와 마찬가지로, 알수 없는 출처로부터 전송된 첨부파일 및 파일을 열지 마십시오. 당신의 기기에 실수로 악성 말웨어를 다운로드 하게되는 가장 쉬운 방법 중 하나입니다.

5) 인터넷에 연결된 모든 기기들에 바이러스 백신프로그램을 설치하십시오. 당신의 태블릿과 휴대전화 또한 포함됩니다. Avast 및 Avira 같이 훌륭한 무료 백신프로그램 또한 존재합니다.

6) 당신의 모든 기기들을 암호화 하십시오. 당신이 안드로이드 휴대기기를 사용하든 윈도우 컴퓨터를 사용하든, 전체 디스크암호화는 보안의 중요한 부분이며 당신의 모든 기기에 활성화해야 합니다. 이 기능은 당신의 기기가 도난당하거나 분실되었을 때 기기 내의 데이터가 노출되지 않도록 보호합니다.

7) 가능한 많은 계정에 2단계 인증을 활성화하십시오. 감청 및 보안위협이 비교적 많은 문자메시지보다 모바일 어플리케이션들을(예: Google Authenticator, Authy) 이용한 2단계 인증을 권장합니다. 2단계 인증의 활성화가 가능한 서비스들은 다음의 웹사이트에서 찾아볼 수 있습니다 - https://twofactorauth.org/

8) VPN을 사용하십시오. 특히, 카페 및 공항과 같이 공격에 취약한 Wifi 네트워크에 접속할 때 VPN을 사용하길 권장합니다. 대부분의 VPN서비스들은 연간 이용료를 지불해야 이용가능한 유료서비스이나, Tunnelbear(https://tunnelbear.com) 와 같이 무료로 소량의 대역폭을 제공하는 서비스 또한 존재합니다.

9) 신뢰할 수 있는 개발자의 응용프로그램만 설치하며, 불법복제된 자료들을 피하시길 바랍니다. 또한 다운로드 후에는 프로그램 및 어플리케이션이 요청하는 권한들에 대해 검토하십시오. 일반적인 게임 소프트웨어가 당신의 사진, 연락처, 이메일, 문서, SNS 게시 권한을 요청해서는 안됩니다.

10) 데이터를 백업하십시오! 2017년에 일어난 일들이 우리에게 가르쳐 준 것이 있다면, 그건 바로 랜섬웨어가 증가하고 있다는 사실입니다. 데이터의 백업들 중 적어도 하나를 완전히 다른 공간 또는 장소(디지털 또는 물리적 외부 공간)에 배치하십시오. 같은 공간(예 - 같은 기기, 같은 저장장치, 같은 사무실)에 3개의 백업데이터를 보관하는 것은 도움이 되지 않습니다. 만약 화재가 발생한다면 모두 잃게 될수 있기 때문입니다.

참고자료:

- https://ssd.eff.org
- https://securityplanner.org