인터넷 컴퓨터 및 휴대폰 사용시 사용자의 개인정보 보호 및 보안을 목적으로 중동 및 북아프리카의 주민들을 위해 작성된 실질적 안내서 (개정판: 2011 년 7 월)

본 안내서는 원래 중동 및 북아프리카 지역의 주민들이 데이터(뉴스 리포트, 정보, 미디어 등)를 안전하게 전달, 관리, 공유할 수 있게 하는 목적으로 작성되었지만 자신의 개인정보 보호 및 보안을 위해 누구나 유용하게 사용할 수 있습니다.
본 안내서는 보통 수준의 컴퓨터 활용 지식을 보유한 사람들을 대상으로 하여 컴퓨터로 인터넷에 접속하거나 또는 휴대폰을 사용할 때 어떠한 조치를 취할 수 있는가를 알려드립니다.
본 안내서는 감시와 모니터링을 받는 가능성을 줄이고, 개인정보를 보호하며, 검열에 대응할 수 있는 유용한 팁과 도구들을 제공해 드립니다.
본 안내서는 안전한 이메일 교신 및 채팅, 비밀번호의 안전한 관리, 바이러스 및 스파이웨어 방지, 신원을 밝히지 않고 온라인 검열을 회피하는 방법, 휴대폰을 안전하게 사용하는 방법을 알려드리며 보다 더 전문적인 정보를 제공해 주는 사이트들의 링크 주소도 알려 드립니다.
(아래에 언급된 우회 도구를 사용한 후에도 차단된 사이트로 인해 이 문서에 기재된 링크로 접속할 수 없는 경우, info@accessnow.org 로 이메일을 보내서 어떤 정보를 이메일로 받기를 원하시는지 알려주시기 바랍니다).
본 안내서에 기재된 모든 정보는 2011 년 7 월자로 정확하다고 간주되지만 신기술과 취약점이 계속 소개되고 발견되는 인터넷상에서 개인정보를 보호한다는 것은 어려운 과제입니다.
인터넷상에서 보안과 사생활 보호를 완벽하게 보장해 줄 수 있는 특효약은 없지만 본 문서에 기재된 도구와 각종 팁을 사용하시는 경우 여러분의 데이터를 보다 더 안전하게 보호하실 수 있습니다.

본 안내서는 온라인 및 이동통신 보안 분야의 여러 단체와 전문가들에 의해 작성되고 동료평가를 받았습니다. 그러나, 본 문서에 오류 또는 개선할 사항을 발견하시는 경우 info@accessnow.org 로 연락해 주시면 대단히 감사하겠습니다.

중요한 기초적 사항:

E-mail 계정을 보호하는 방법:

무료로 제공되는 가장 널리 사용되는 이메일중 Hotmail 과 Gmail 은 사용자와 이메일 서비스 제공자간에 암호화된 연결 서비스(HTTPS)를 제공합니다.

Gmail 의 경우 HTTPS 가 디폴트로 선택이 되지만 Hotmail 의 경우 이미 HTTPS 를 사용하도록 이미 설정되지 않았으면 (계정 > 기타 옵션 > HTTPS 로 자동연결)을 선택하시기 바랍니다.
현재 Yahoo 이메일 계정은 보안이 되지 않기 때문에 불편하더라도 HTTPS 보안 연결을 사용하는 이메일 계정을 열어 사용할 것을 추천하는데 이것은 민감한 정보를 주고 받는 경우 더욱 중요합니다. 그러나 HTTPS 보안연결은 사용자와 이메일 제공자간의 연결만 보안해 주기 때문에 수신자가 HTTPS 를 사용하지 않거나 또는 다른 이메일 제공자를 사용하는 경우 이메일이 최종 목적지로 배달되는 과정에서 이메일이 암호 해제되어 데이터가 노출될 수 있습니다. Riseup.net 및 Vaultletsoft 도 역시 보안된 이메일 서비스를 제공합니다. 추가적으로, PGP 및 GPG 는 이메일의 암호화 및 디지털 서명에 사용될 수 있는 우수한 시스템입니다 (이에 대한 자세한 설명은 영어 및 아랍어로 읽으실 수 있습니다).

다른 보안기능(보안인증, IP 역사)에 대해 알고 싶은 Gmail 사용자들은 Gmail Security Checklist 를 참조하십시오. Hotmail 사용자로서 공용 컴퓨터에서 사용할 수 있는 1 회용 암호번호 등의 보안 기능에 대해 보다 자세한 정보를 원하시는 경우 여기를 누르십시오.

보다 더 안전한 비밀번호 만드는 방법:
강력한 비밀번호를 만들고 유지하는 것은 절대적으로 중요하며 이를 위한 유용한 팁은 다음과 같습니다:

- 단어 하나 보다는 구절을 사용하십시오.
- 12 자 또는 그 이상 길이의 비밀번호를 선택하면 소프트웨어로 비밀번호를 깨기가 더 어렵습니다.
- 특수문자, 숫자, 대문자 및 소문자를 섞어 사용하십시오. 속담 또는 노래나 시의 한 구절의 단어나 문자를 특수문자나 숫자로 대치하는 것도 좋은 방법의 하나입니다.
- 모든 계정에 같은 비밀번호를 사용하지 마십시오; HTTPS 보안연결이 되지 않은 곳에서 사용한 비밀번호를 보안연결된 곳에서 사용하면 그 비밀번호가 해킹된 후 보안된 계정에 사용될 수 있습니다.
- 정기적으로 3 개월 마다 비밀번호를 바꾸고, 인터넷 카페 또는 자신의 컴퓨터가 아닌 컴퓨터를 사용하는 경우에는 비밀번호를 더 자주 바꾸십시오.
- 비밀번호를 기억하기 어려우면 KeePass 또는 유사한 보안된 프로그램을 사용하면 도움이 될 수 있습니다.
- 일부 경우에는 잊은 비밀번호를 복구시켜 주는 시스템을 통해 계정이 해킹되기도 합니다. 귀하의 계정에 대한 보안 질문과 답은 간단하거나 또는 정답을 주기가 쉽지 않아야 합니다.

안티바이러스 및 안티스파이웨어:
대부분의 컴퓨터 사용자들이 가지고 있는 가장 큰 문제는 불법복제 소프트웨어를 사용하는 것인데 마이크로소프트 윈도우즈가 특히 그렇습니다. 불법 소프트웨어를 사용하는 경우 얼마의 돈은 절약할 지 모르지만 소프트웨어 제작사로 부터 업데이트나 패치를 받지 못하는 위험이 따르게 됩니다. 만약에 공식적이고 합법적인 소프트웨어 또는 운영체계를 구입할 수 없는 경우, 리스크를 최소한으로 줄이기 위해 효율적인 안티바이러스 및 안티스파이웨어를 설치해야 합니다.
그러나 귀하의 데이터의 안전을 위해 가급적이면 정품 소프트웨어를 사용하기 바랍니다.

- 효율적인 윈도우즈용 안티바이러스 프로그램을 이미 사용하지 않는 경우 Avast 프로그램이 여러분의 컴퓨터에 있는 데이터에 손상이 가거나 감염되지 않도록 보호해 줄 수 있습니다. 여러분의 컴퓨터가 이미 감염된 경우에는 안전모드에서 Malwarebytes 프로그램을 실행할 수도 있습니다.
- 여러분의 모든 온라인 및 오프라인 활동을 추적하는 악성 소프트웨어를 추적하고 제거하는 안티스파이웨어 프로그램을 설치하는 것도 역시 중요한데 Spybot 은 효율적인 무료 안티스파이웨어 프로그램의 하나입니다.
- 바이러스나 스파이웨어를 막으려면 모르는 사람 또는 신뢰할 수 없는 출처의 이메일이나 첨부물을 열지 않아야 합니다. 첨부물, 파일을 보낸 사람이나 웹사이트를 잘 알지 못하는 경우 VirusTotal 로 업로드하여 테스트하거나, 또는 제목란에 “SCAN”이라고 기재하고 scan@virustotal.com 로 이메일을 보내주시면 됩니다 (테스트 결과를 XMS 포맷으로 원하시는 경우 “SCAN+XML”이라고 제목란에 기재하십시오).
- 악성 코드에 감염되는 다른 흔한 경로의 하나는 웹을 브라우징하다가 악성 코드에 감염되는 것입니다. Firefox 를 사용하는 경우, 대부분의 스크립트를 차단시키고 신뢰하는 사이트에만 액세스를 허용해 주는 NoScript 를 다운로드해서 사용하실 것을 강력히 추천합니다.
- USB 스틱 또는 다른 리무버블 장치로 부터도 바이러스가 감염되기 쉽습니다. 이미 잘 알려져 있고 신뢰할 수 있는 사이트에서 온 경우에만 귀하의 컴퓨터에 리무버블 장치를 연결하십시오. Spybot 또는 Avast 같은 안티바이러스나 안티스파이웨어 프로그램을 사용하여 리무버블 장치를 스캔하십시오.

윈도우즈를 계속해서 사용해야하는 특별한 이유가 없는 경우 Ubuntu 라는 리눅스 시스템으로 마이그레이션하는 것을 고려하십시오. 우분투는 디폴트로 암호화된 하드 드라이브를 사용할 수 있게 하며 근본적으로 바이러스나 악성웨어가 없습니다. 우분투 사용자는 타겟 공격을 받는다 하더라도 업데이트 패치를 설치하지

않았거나, 무단복제 또는 구식 윈도우즈를 사용하는 사용자 보다 훨씬 더 안전합니다. 리눅스 Mint 는 우분투에 기반한 운영체계로서 여러 종류의 응용프로그램을 사용할 수 있습니다.

보안된 인스턴트 메시징:
귀하의 계정이 해킹의 표적이 되지 않을 것이라고 생각하시는 경우, HTTPS 보안이 된 Gmail 안에서 Skype 또는 Google Chat 을 하는 것이 좋은 방법입니다. 그러나 이 보다 훨씬 더 안전한 방법은 Pidgin 과 Off The Record (OTR) 플러그인을 사용해서 Google Talk 등의 채팅 프로그램을 액세스 하는 것입니다 --
Privacy by Design 에 기재된 내용을 이해하려면 OTR's security properties (OTR 의 보안 속성)을 상세히 읽으십시오.

온라인에서 컴퓨터를 보호하는 방법:

- 온라인 활동가 일을 할때 소셜 네트워크 및 미디어 사이트에서 신원을 밝히라는 요청이 들어오면 신원을 감추기 위해 별칭을 만들어 사용할 수 있습니다. 어느 정도로 익명을 사용할 것인가는 여러분의 결정에 달려있습니다: 많은 사람들은 트위터에서 익명을 사용하지만 페이스북 같은 소셜 네트워킹 사이트에서는 대부분의 사람들이 실명을 사용합니다. 실명을 사용할 것인가 익명을 사용할 것인가는 본격적인 온라인 감시를 당할 가능성과 여러분의 판단에 달려있습니다.
- 페이스북의 경우, 예를들어 단어 하나로 구성된 것 같은 분명히 익명이라고 알 수 있는 이름으로 등록된 계정은 서비스 제공 조건을 위반한다는 이유로 계정이 삭제될 수 있음으로 실감나는 익명을 사용해야 합니다. 페이스북에서 실명을 사용하고 HTTPS 를 통해 페이스북을 액세스하거나 사용하기로 결정한 경우 전화번호 같은 추가적인 중요한 개인 신상정보를 제공하지 않는 것이 중요합니다.
- GPS 기술을 사용하여 사용자의 실제 위치를 활용하는 온라인 프로그램이 날로 증가하고 있습니다. 이 기능은 위기 또는 중대한 사건이 발생할때 휴대폰을 사용해서 현장에서 들어오는 보고들을 관리하는 강력한 도구로 사용될 수 있지만, 이와 동시에 사용자의 위치 및 활동같은 매우 중요한 정보를 외부로 노출시킬 수도 있습니다. 저희들은 일시적르호나 또는 활동가의 프로젝트 목적상 불가피한 경우를 제외하고는 트위터나 Bambuser 같은 프로그램의 GPS 트래킹 기능을 끌것을 추천합니다. GPS 를 디스플레이하지 않더라도 사용자의 웹브라우저나 또는 다른 클라이언트들이 귀하의 위치정보를 수집하지 못하게 GPS 기능을 비활성화시키는 것이 절대적으로 중요합니다.
- 중요한 정보를 다른 사람에게 보낼 때 그 정보의 수신자들이 보안되지 않았으면 그들의 연락처, 이메일 또는 기타 통신이 감시될 수 있다는 사실을 명심하시기 바랍니다. 신원을 확인하지 않은 사람들과 통신을 할때도 각별한 주의가 필요합니다. 또한, 페이스북 또는 트위터를 통해 아는 사람 또는 모르는 사람에게 직접 보내는 메시지도 수신자가 필요한 조치를 취하지 않은 경우 그 메시지 내용을 제 3 자가 읽을 수 있습니다 (우측에 있는 HTTPS 및 감시회피 도구에 대한 추가적 정보를 참조하십시오).
- 귀하의 계정을 액세스하는 서드파티 앱을 최소한으로 줄이거나 또는 전혀 사용하지 마십시오 (예: 트위터, 페이스북, Gmail 등을 위해 귀하의 계정을 액세스하는 앱). 이러한 앱은 종종 보안성을 위협할 수 있으며 보안된 다른 계정을 침입하는 목적으로 사용되기도 합니다.

온라인 보안:
바레인, 쿠웨이트, 오만, 카타르, 시리아, 사우디아라비아를 포함한 중동 및 북아프리카의 여러 국가에서는 인터넷 검열이 심하게 진행되고 있습니다. 어느 정도로 심한지는 모르지만 인터넷 감시도 되고 있습니다. 검열을 회피한다는 것과 감시를 회피한다는 것은 같은 것이 아니며 감시를 회피하는 것은 더 어렵습니다. 그러기 위해서는 귀하의 행동이 감시, 기록된다는 가정하에 보안된 무명 프록시를 사용하도록 노력해야 합니다. 또한, 인터넷 익스플로러는 취약점이 많기 때문에 사용하지 않도록 저희들은 강력히 추천하는데 불법복

제된 인터넷 익스플로러의 경우 더욱 그러합니다. 무료로 제공되는 모질라 Firefox 는 좋은 대용 프로그램이며 다수의 유용한 애드온을 제공해 줍니다.

HTTPS 를 사용해서 귀하의 온라인 활동을 암호화하는 방법:
귀하가 온라인 행동주의에 관련하는 경우 신분과 암호를 안전하게 관리하는 것이 중요합니다.
저희들은 최근에 튀니지아에서 온라인의 취약성을 이용하여 대대적인 피싱 캠페인을 벌리는 것을 목격했습니다. 그러나 다행히도 페이스북이 HTTPS 를 인에블해서 도움이 되기는 했었습니다.
가능한한 언제나 HTTPS 를 사용하시기 바랍니다. HTTPS 를 사용할 수 없는 경우 다른 종류의 보안된 프록시 시스템을 사용하는 것이 절대적으로 중요합니다. 검열 행위는 특정된 사람들 또는 사이트들을 상대로 적용될 수 있으며 HTTPS 사이트들에 액세스하지 못하게 하기도 합니다.
TOR 와 같은 익명 프록시를 사용하는 경우, 감시기관이 그러한 표적 공격을 하기가 매우 힘들거나 또는 불가능합니다.

HTTPS:
HTTPS Everywhere 는 사용하기가 쉽고 훌륭한 애드온이기 때문에 저희들이 강력히 추천드립니다.
이것은 Firefox 애드온으로서 가능한 경우 언제나 HTTPS 를 사용하게 합니다. **페이스북, 트위터, 구글 서치 등에서 종단간(End-to-End) 암호화를 하려고 할 때 제일 먼저 해야 하는 일의 하나는 이것을 다운로드하는 것입니다.** 이것은 또한 오픈 또는 보안되지 않은 wifi 네트워크를 공유할 때 암호를 포착 당할 수 있는 위험을 감소시켜 줍니다. 최신 Firefox 버젼을 가지고 있지 않으신 경우 가장 최신 버젼의 Firefox 를 다운로드하십시오.

- 그리고는 HTTPS Everywhere 및/또는 Force TLS 를 다운로드하고, Firefox 를 새로 시작한 후 선호사항을 선택하십시오. 주의사항: HTTPS Everywhere 에는 사용자 정의가 가능한 다수의 디폴트 사이트들이 있습니다. Force TLS 는 HTTPS 를 강제로 사용하게 하는 사이트들의 목록을 사용자가 만들 수 있게 함으로 사용자가 지정할 사항들이 더 많습니다.
- Google Chrome 을 사용하시는 경우 KB SSL Enforcer Extension 을 다운로드 하십시오. (주의 사항: 이것은 위에 언급된 Firefox 의 애드온처럼 효과가 좋지는 않습니다. SSL Enforcer 에는 아직도 버그가 어느정도 있지만 시간이 지나며 더 향상될 것입니다.)

페이스북: 위에 언급된 Firefox 애드온은 많은 사이트에서 HTTPS 를 사용하도록 하지만 페이스북을 자주 사용하는 경우 페이스북이 디폴트로 HTTPS 를 사용하게 설정하는 것이 바람직한데 다수의 컴퓨터로 부터 페이스북을 액세스하는 경우 특히 편리합니다.

- HTTPS 로 페이스북을 접속하려면 화면의 상단 우측에 있는 "계정"에서 "계정 셋팅"을 선택하고, 셋팅 탭에서 계정 보안 "변경"을 선택한 후, “보안 브라우징 (HTTPS)”을 체크하십시오.
- 일부 게임 또는 다른 페이스북 애드온을 사용하면 HTTPS 가 비활성화됩니다.
- 페이스북에는 이제 remote log-out 및 사용자의 계정을 액세스 할 수 있는 디바이스 수를 제한할 수 있게 하는 log-in notifications 같은 다른 보안 기능들이 포함돼 있습니다. 페이스북의 보안 기능을 보여주는 video 는 페이스북 사이트에서 볼 수 있습니다. 페이스북을 안전하게 사용할 수 있는 포괄적인 안내서는 여기를 클릭해도 보실 수 있습니다.

트위터: 위에 언급된 Firefox 애드온이 트위터에서도 HTTPS 를 사용하게 하지만 트위터 자체가 디폴트로 HTTPS 를 사용하도록 설정하는 것이 더 바람직한데 여러 컴퓨터 또는 공공 컴퓨터에서 트위터를 액세스하는 경우 특히 더욱 그러합니다

- 트위터에서 HTTPS 를 사용하려면 화면의 우측 상단에 있는 트위터 핸들을 클릭하고, '셋팅'에서 화면의 하단으로 스크롤한 후 '항상 HTTPS 사용' 상자를 클릭하십시오.

- 주의 사항: 현재로는 트위터 계정에서 '항상 HTTPS 사용' 이라고 설정하더라도 현재로는 이동장치에서도 HTTPS 를 강제로 사용하게 하지는 못합니다. 이 문제가 해결될 때 까지는 항상 https://mobile.twitter.com 를 사용하시기 바랍니다.

우회 방법: 차단된 사이트를 방문하는 방법

중동 및 북아프리카 지역의 여러 국가들은 다수의 사이트 및 블로그에 대한 대규모 필터링을 시행하고 있는데 필터링을 하는 수준은 국가마다 다르지만 대규모의 필터링이 시행되고 있다는 사실은 고수준의 감시도 진행되고 있음을 암시한다고 생각해도 무리가 아닐것입니다.
블록된 사이트로 미디어를 업로드하려면 우회 도구를 사용해야 합니다.
암호화하는 것과 개인정보를 보호하고 무명화하는 것에는 차이가 있다는 것을 인지하는 것이 중요합니다: 좋은 우회 도구들은 사용자와 우회도구 제공자간의 통신을 암호화합니다. 그렇다 하더라도 우회도구들은 우회도구 제공자와 방문하는 사이트간의 통신은 비밀화하지 못합니다.
HTTPS 는 종단간(End-to-End) 암호화를 제공해 주는데 그렇기 때문에 가능한 한 언제나 HTTPS 를 사용하는 것이 중요합니다. 그러나 HTTPS 자체는 블록된 사이트를 액세스 할 수 있게 만들지 못하기 때문에 우회도구를 사용하는 것이 필요합니다.
원격 서비스는 항상 귀하의 IP 주소를 저장합니다 - 따라서, Tor 와 같은 무명화 프록시를 사용하는 경우에만 사용자의 IPO 주소를 실질적으로 안전하게 감출 수 있습니다.
많은 서비스들이 귀하의 과거 로그인 정보들을 알려주기 때문에 귀하의 계정이 해킹당하는 경우 귀하의 과거 위치가 알려지게 됩니다.

방화벽을 우회하는 방법

단순한 웹 기반 프록시들은 웹 페이지 폼(form)을 통해 블록된 사이트를 액세스하게 해줍니다.
사용자들이 프록시 사이트로 가서 방문하려는 사이트의 URL 을 입력하면 그 프록시가 그 페이지를 가져와서 사용자의 화면에 디스플레이해 줍니다. HTTP/SOCKS 프록시들은 방화벽을 뚫고 갈 수 있게 하는 프로토콜을 통해서 웹 트래픽이 통과하게 합니다. 공공 프록시 디렉토리 사이트에 기재된 IP 주소 및 포트 번호가 브라우저의 구성에 입력됩니다.
필터링을 우회하기 위해 웹 기반의 간단한 프록시 및 HTTP/SOCKS 프록시가 종종 사용되지만 이들은 무명성을 제공해 주지 못하며 (즉, 사용자의 웹 사용 정보를 보거나 감시할 수 있음) 대부분의 경우, 누가 익명성을 제공하는지 알 수 없습니다.
이러한 방법은 많은 리스크를 동반함으로 우회기능 및 무명성을 제공해 줄 수 있는 Tor 와 같은 시스템을 사용할 것을 권장합니다.

프록시 기반 솔루션의 하나인 Psiphon 도 고려해 볼 가치가 있습니다. Psiphon 은 여러가지 다른 형태로 제공됩니다. Psiphon 1 은 경량급 웹 프록시로서 MS 윈도우즈 및 리눅스 컴퓨터에서 사용됩니다. 일반적으로 말해, 싸이폰 노드(Psiphonodes)들은 개방된 공공 프록시가 아닙니다.
이들의 목적은 특수 컴퓨터 하드웨어를 가지고 있지 않은 일반인들이 웹 사이트를 블록하는 국가에 있는 소수의 '동료'들에게 프록시 기반의 우회 기능을 제공할 수 있게 하는데 있습니다.
싸이폰 프록시를 제공하는 '동료'들은 그들의 싸이폰모드를 지나가는 모든 인터넷 트래픽을 액세스할 수 있기 때문에 싸이폰노드 제공자와 인터넷을 검열하는 국가에서 그러한 노드를 사용하는 유저들이 서로 신뢰할 수 있는 관계를 가져야하는데 그렇기 때문에 싸이폰 프록시를 신뢰의 웹(web-of-trust)이라고 부르기도 합니다. **싸이폰은 사용자에 대한 데이터를 기록합니다. 그러나 IP 주소는 무명화됩니다.** Psiphon 2 는 Psiphon 사가 경영하는 중앙집중 관리형의 클라우드 솔루션으로서 링크를 덮어쓰는 프록시로 구성돼 있습니다. Psiphon 1 및 2 는 HTTPS 및 Web 2.0 사이트를 다루는데 문제가 있습니다. 그러나 신버전인 PsiphonX 에서는 그러한 문제들이 해결되었습니다.

Tor: 온라인 익명성

Tor 는 인터넷 필터링을 우회할 수 있게 해주는 우수한 기능을 가진 훌륭한 도구이며 익명성을 보호해 주는 인터넷 커뮤니케이션 시스템입니다. Tor 의 가장 큰 단점은 다른 방법에 비해 웹 브라우징 속도가 떨어질 수 있다는 것입니다.

Tor Browser Bundle 은 모든 셋업 작업을 처리해 주며 Tor Bridge 를 사용하여 필터링이 심한 국가에서도 원하는 사이트를 액세스를 할 수 있게 도와줄 수 있습니다. Tor 를 사용하는 방법은 여러가지가 있지만 저희들은 Tor Browser Bundle 을 우선 다운로드 하실 것을 권장하는데 그 이유는 토르 브라우저 번들을 사용하면 Windows, Mac OS X, 및 Linux 에서 각각 다른 프로그램을 설치할 필요가 없기 때문입니다. 토르 브라우저 번들을 실행하면 커스텀화된 Firefox 와 Vadalia 가 시작되는데 Vidalia 는 토르 컨트롤러 프로그램으로서 토르 네트워크로 연결한 후 모든 트래픽을 그 네트워크를 통해 연결하고 보내도록 미리 설정돼 있습니다. 토르 브라우저 번들을 USB 플래시 드라이브에 설치하면 다른 컴퓨터에서도 토르 브라우저 번들을 사용할 수 있습니다. 보안이 돼있거나 또는 되지 않은 여러 종류의 언어(아랍어 및 페르시아어 포함)로 된 인스턴트 메시지용 브라우저 번들을 사용하려면 Tor download site 를 방문하십시요. 토르를 사용하는 경우 웹 브라우징 속도가 느려질 수 있음으로 브라우저를 두개 사용하여 민감하거나 또는 차단된 정보를 액세스 할 때는 토르를 사용하고 민감하지 않은 웹 브라우징을 할 때는 보통 브라우저를 사용하실 것을 추천합니다. 토르를 계속 연결해 두면 시간이 흐름에 따라 전송 효율이 증가되면서 전송속도가 빨라지는 것을 느낄 수 있습니다. 토르를 사용해서 웹사이트를 액세스하는 속도가 너무 느리고 보려는 내용이 주로 텍스트인 경우, 브라우저에서 이미지와 자바 스크립트를 턴 오프할 수 있습니다. 이러한 경우, 토르를 통해 페이지를 로딩하는 속도가 대폭 증가할 수 있습니다.

그러나 불행히도 위의 토르 메인 웹사이트는 중동 및 북아프리카 지역의 대부분의 국가에서 차단되고 있습니다. 그러나 아직도 아래의 사이트에서 이 소프트웨어를 액세스 할 수 있습니다:

- HTTPS 를 사용해서 토르 웹사이트로 가기 - https://www.torproject.org/
- 구글에 "tor mirror"를 입력해서 torproject.org 미러 사이트를 찾음. 또한, 구글로 "site:torproject.org mirrors"를 찾아서 "Tor Project: Mirrors" 페이지로 가면 공식 미러 사이트들을 찾을 수 있습니다.
- 또는, gettor@torproject.org 로 이메일을 보내면 "gettor" 로봇으로 부터 번들을 받을 수 있습니다. 참고사항: gettor@torproject.org 로 이메일을 보낼때 최고 수준의 보안을 유지하려면 HTTPS 보안이 유지되는 Gmail 을 사용하십시오. 아래의 목록에서 원하시는 번들을 하나 골라서 귀하가 보내는 이메일의 아무런 곳에나 기입하십시오.
  - 윈도우즈용 tor-im-browser-bundle (Tor 및 인스턴트 메시징)
  - 윈도우즈 또는 인텔 Mac OS X 또는 Linux 토르-브라우저-번들 (Tor browser 용)

이메일을 보낸 잠시후 "Gettor" 로봇이 요청하신 소프트웨어를 귀하에게 zip 파일로 보내드릴 것입니다. 토르에 대한 더 상세한 정보를 원하시면 tor-assistants@torproject.org 로 연락 주시기 바랍니다.

토르는 또한 안드로이드 전화에서 "Orbot"이라는 이름을 통해 다운 받으실 수 있습니다.
이 앱은 안드로이드 시장을 검색하거나 또는 토르 웹사이트 또는 미러 웹사이트에서 직접 다운받을 수 있습니다. 통신 내용을 암호화 하고 익명성을 제공해 주는 또 다른 우회 방법의 하나는 VPN 네트워크를 사용하는 것입니다. VPN 네트워크를 셋업하는 자세한 설명을 받으시려면 여기를 클릭하면 되며, 무료 버젼의 VPN Hotspot Shield 를 다운 받으려면 여기를 클릭하거나, 또는 hss-sesawe@anchorfree.com 로 이메일을 보내면 됩니다 (이메일의 제목란에는 반드시 "hss", "sesawe", "hotspot" 또는 "shield" 중 최소한 하나의 단어가 포함돼야 합니다.).

널리 사용되는 다른 우회 도구로는 Ultrasurf 및 Freegate 등이 있습니다.
위에 기재된 3 개의 VPN 들은 차단된 사이트를 액세스하는 좋은 도구이지만 간단한 웹 프록시 및

HTTP/SOCKS 프록시들이 그렇듯이 익명성을 제공해 주지 못한다는 점을 고려하는 것이 중요합니다 (즉, 차단된 사이트를 액세스할 때 귀하의 신원을 감추지 않습니다). 추가적으로, 위의 서비스들은 그들의 운영자들이 지지하지 않거나 또는 좋아하지 않는 사이트들을 필터링해서 차단하는 것으로 알려져 있습니다. 뿐만아니라, 이러한 사이트들은 모든 사용자의 데이터를 기록하는 것으로 알려져 있습니다. 이들은 사용자의 개인적 정보 (방문하는 사이트, 검색용어 등)에 의거한 맞춤 광고를 사용자에게 제공하여 수익을 얻는 영리적인 사업체인데 이것은 익명성 또는 단순히 프라이버시를 위해 우회 소프트웨어를 사용하는 경우 반드시 고려해야 할 사항입니다.

중요 사항: 인터넷 서비스를 컨트롤하는 국가의 정부는 컴퓨터 프로그램 또는 보안 인증서와 같은 여러가지 전략을 사용해서 사용자의 보안과 프라이버시를 침해할 수 있습니다. 이러한 행동에 대응하려면 일부 정부의 이러한 행위를 적발하고 조기 경보를 주는 온라인 행동가들이 제공하는 뉴스와 경보사항을 계속 청취하도록 노력해야 합니다.

추가적 정보: Video tutorials 은 여러 종류의 우회 도구를 영어 또는 아랍어로 제공해 줍니다 (12 pm Tutorials).

이동통신 장치

많은 활동가들은 그들의 휴대폰을 통해 추적을 당하는데 일부 국가는 다른 국가보다 더 심하게 감시를 시행하고 있습니다. 이집트의 활동가들은 모든 면에서 높은 수준의 감시를 받았는데 이집트의 정보당국은 통화중도 아닌 전화를 원격으로 조절하여 도청 장비로 사용하는 것 같은 기술들을 사용했습니다. 따라서, 귀하는 귀하의 국가에서 어떤 감시 활동이 시행되고 있고, 귀하가 하는 일이 얼마나 중요하며, 또한 다른 활동가들이 어떤 종류의 감시를 당하고 있는가를 고려하여 귀하의 리스크를 평가해야 합니다. 전화회사는 고객의 위치를 포함한 고객의 휴대폰에 관련된 정보를 추적하고 수집할 수 있는 능력을 가지고 있으며 정부가 요청하는 경우 그러한 정보를 정부에 제공해 줄 수 있습니다.

사용자가 모르게 휴대폰에 백그라운드로 실행되는 감시 프로그램이 설치될 가능성도 있습니다. 귀하가 귀하의 휴대폰을 몸에 항상 휴대하고 있지 않는 한 이러한 프로그램이 자신도 모르게 설치될 위험이 존재합니다.

휴대폰이 켜져 있으면 휴대폰은 계속해서 근처에 있는 휴대폰 안테나 마스트에게 다음과 같은 정보를 보냅니다:

- IMEI 번호 - 휴대폰 하드웨어의 고유한 번호
- IMSI 번호 - 휴대폰에 있는 SIM 카드의 고유한 번호
- TMSI 번호는 사용자의 위치 또는 안테나의 작동범위에 따라 수시로 임시적으로 재할당되지만 시판되고 있는 도청 시스템으로도 추적이 가능합니다.
- 휴대폰이 작동하는 네트워크 셀의 크기는 도심지의 경우 불과 몇 미터로 부터 시외의 경우 여러 평방 킬로미터에 달하는 지역일 수 있는데 일부 빌딩의 경우 실내의 신호 강도를 향상시키기 위해 반복기 안테나를 사용하기도 합니다.
- 네트워크 셀 안에 있는 휴대폰 사용자의 위치는 근처의 안테나 마스트들에서 받는 신호를 삼각 측량법으로 찾아낼 수 있습니다. 다시 말하면, 휴대폰의 위치를 얼마나 정확하게 알아낼 수 있는가는 셀의 크기에 달려있는데 해당 지역에 마스트가 많이 있을 수록 더 정확한 위치를 알아낼 수 있습니다.

그렇기 때문에 귀하의 휴대폰이 켜져 있어서 네트워크 마스트와 통신하고 있으면 통신회사가 수집하는 정보를 액세스할 수 있는 사람들이 귀하의 휴대폰을 감시도구로 사용할 수 있게 되는데 이런 식으로 그들이 액세스할 수 있는 정보는 다음과 같습니다:

- 사용자가 송수신한 전화통신에 대한 정보

- 송신자 및 수신자의 정보를 포함한 문자 메시지 내용
- 사용자가 사용한 데이터 서비스 (예, HTTPS 를 사용하지 않은 경우에는 모든 웹 브라우징 활동 내력, 보안되지 않은 인스턴트 메시징) 및 전송한 데이터의 볼륨 (즉, YouTube 로 비디오를 업로드했는가?)
- 사용자의 대략적인 위치 (안테나 타워의 밀도에 따라 수 미터에서 수 킬로미터에 달함)

감시를 당하고 있다고 생각할 때 SIM 카드만 바꾸면 감시를 피할 수 있다고 생각할 지 모르지만 사실은 휴대폰 또는 기타 이동통신 장치 자체의 고유번호 (IMEI)를 통해서도 추적 당할 수 있음을 명심해야 합니다.

귀하의 휴대폰이 압수되거나, 도난 또는 분실된 경우 귀하의 휴대폰에 내장된 정보들이 귀하에게 불리하게 사용될 수 있습니다. 모든 휴대폰에는 자체에 내장된 메모리 이외에도 SIM 카드에 소량의 메모리가 있습니다. (또한 일부 휴대폰에는 멀티미디어 파일 저장용으로 SD 또는 micro SD 카드가 있습니다.) **일반적으로 말해 휴대폰에 내장된 메모리에 데이터를 저장하는것 보다는 SIM 카드 또는 SD 메모리 카드에 저장하는 것이 더 바람직한데 그 이유는 SIM 또는 SD 카드에 저장된 정보는 이동 또는 파괴하기가 더 쉽기 때문입니다.** SIM, 휴대폰 내장 메모리, 그리고 SD 메모리 카드 (해당되는 경우)에 저장되는 정보는 다음과 같은 항목을 포함합니다:

- 휴대폰 전화번호부 - 연락처 이름 및 그들의 전화번호
- 통화내역 - 귀하가 전화를 건 사람 및 귀하에게 전화를 건 사람 및 통화 시간
- 송신 또는 수신한 SMS
- 칼린더 및 할일 같은 프로그램의 데이터
- 휴대폰으로 찍은 사진 또는 비디오. 대부분의 휴대폰은 사진을 찍은 시간 및 사진을 찍은 위치도 저장할 수 있습니다

웹 브라우징 기능이 있는 휴대폰을 소유한 경우 귀하의 브라우징 내역이 얼마나 휴대폰에 저장돼 있는가를 고려해야 합니다. 가능한 경우 브라우징 내역을 저장하지 마십시오.
감시기관이 귀하의 SIM 카드나 휴대폰 메모리를 액세스하는 경우 저장된 이메일 내용도 읽을 수 있는 위험이 있습니다.

컴퓨터의 하드드라이브 처럼 SIM 메모리에 일단 데이터가 저장되면 SIM 이 꽉 차서 가장 오래된 데이터가 겹쳐 써질 때 까지 물리적으로 그 데이터가 남아 있게 됩니다.
이것은 즉 문자 메시지, 통화 기록 또는 연락처 정보를 삭제하더라도 SIM 카드로 부터 그러한 정보를 복구할 수 있는 가능성이 존재한다는 것을 의미합니다
(스마트카드 리더를 사용해서 SIM 카드에 저장된 정보를 복구하는 무료 프로그램이 있습니다).
이와 마찬가지로 휴대폰에 내장된 메모리 또는 메모리 카드에 저장된 정보도 삭제한 후에 복구할 수 있을 가능성이 있습니다.
일반적으로 말해, 휴대폰 메모리가 클 수록 삭제된 정보를 복구할 수 있는 기간이 늘어납니다.

이러한 사실은 무엇을 뜻합니까?
휴대폰은 활동가들에게 강력한 도구가 될 수 있지만, 귀하를 추적하기 위해 정부나 보안기관이 텔레콤 회사와 적극적으로 협력하는 경우 엄청난 리스크를 초래할 수 있습니다. **귀하의 국가에서 휴대폰에 대한 감시가 매우 심하고, 특히 귀하가 어떤 하이프로파일 활동에 관련돼 감시의 대상이 되었다고 생각하는 경우 휴대폰을 사용하지 않을 것을 추천합니다. 직접 사람들과 만나서 미팅을 할 것을 추천합니다.**

어느 정도의 리스크를 감수할 것인가는 귀하의 판단에 달려있습니다: 만약에 귀하가 활동가로 주목받거나 또는 대규모 감시 캠페인의 대상의 하나라고 생각하지 **않는** 경우 휴대폰으로 다른 활동가들과 통신하거나, 사진 및 비디오를 찍거나 또는 정보를 전달하려면 다음과 같은 방법을 사용할 수 있습니다:

- 사전에 약속한 암호를 사용해서 다른 활동가들과 통신함
- 사전에 정한 '전화울리는 횟수' 시스템을 사용함 (예를들면, 전화를 한번이나 두번 울리고 끈는 방법을 사용해서 다른 활동가에게 어느곳에 도착했다는 것을 알리는 등.)
- 주소록에 다른 활동가의 이름을 적을때 숫자 또는 익명을 사용하십시오. 이런 조치를 취하면 만약에 보안기관이 귀하의 전화 또는 SIM 카드를 압수하더라도 그들이 동료 활동가들 모두의 신원을 파악할 수 없게 할 수 있습니다.
- 보안원들이 항의 시위에 참가하는 사람들의 휴대폰을 압수한다는 것을 아는 경우, 시위에 참가할 때 백업 SIM 카드 및 실지로 사용할 수 있는 휴대폰을 가지고 가는 것이 중요합니다. SIM 카드를 없애야 하는 경우 물리적으로 파괴하는 것이 좋습니다.
- 비밀번호로 휴대폰을 잠글 수 있는 경우 그 기능을 사용하십시오. 같은 비밀번호를 SIM 카드의 PIN 번호로 사용할 수도 있습니다. SIM 카드와 함께 제공되는 디폴트 PIN 번호를 다른 번호로 바꾸고 SIM 카드를 PIN 으로 잠그는 기능을 활성화 하십시오. 그러면 휴대폰을 사용할 때 마다 비밀번호(PIN 번호)를 입력해야 합니다.
- 항의 시위에서 보안원들이 강경한 조치를 취할 것이라고 생각하는 경우 휴대폰을 비행기모드로 돌리는 것을 고려할 수도 있습니다. 그렇게 하면 비록 전화를 걸거나 또는 받지는 못하더라도 비디오나 사진을 찍어서 후에 온라인 사이트들에 업로드할 수 있습니다. 이와같은 전략은 어떤 이벤트에서 보안원들이 휴대폰을 소지한 사람들을 전부 단속하는 경우 유용하게 사용할 수 있습니다. 그 이유는, 후에 정부가 어떤 특정된 시간에 특정된 장소에 있었던 모든 사람들의 통화 및 SMS 데이터를 요청해서 집단구속을 할 수 있기 때문입니다.
- 어떤 이벤트에 대한 비디오를 만들때 지오태깅 정보를 포함시킬 필요가 있지 않는 한 각종 에플리케이션의 위치트래킹 및 지오태깅 옵션을 턴오프하십시오. 셀폰으로 비디오를 라이브로 스트림할 때 GPS/지오태깅 옵션을 턴오프하십시오(Bambuser 사용법 참고)
- 안드로이드 휴대폰을 사용하시는 경우 Guardian Project 또는 Whispersys 에서 제공하는 여러가지 도구들을 사용해서 웹 부라우징, 인스턴트 메시징, SMS 그리고 음성통화를 암호화할 수 있습니다.
- 휴대폰으로 웹브라우징을 하는 경우 가능한한 HTTPS 를 사용하십시오.

블랙베리 사용자의 주의사항

블랙베리의 메이커인 Research in Motion (RIM)사는 사용자가 원하는 암호화 수준에 따라 두가지 종류의 계정을 제공해 줍니다. 일반 개인 고객용 블랙베리 계정은 진정한 엔드-투-엔드 암호화 서비스를 제공하지 않으며 RIM 사 또는 이동통신서비스제공업체가 언제나 고객의 통화, 이메일, SMS, 웹브라우징 등을 도청할 수 있습니다. 한편, 블랙베리 엔터프라이즈 서버 (BES)를 사용하는 기업계정 고객들은 이메일, 메신저 (BBM), 및 웹브라우징을 할 때 엔드-투-엔드 암호화 서비스를 제공받습니다. 어쨋건, 기업계정 사용자의 경우에도 해당 회사의 IT 관리자는 사용자의 암호화된 모든 통신 내용을 해독할 수 있는 도구를 가지고 있으며 많은 정부들은 합법적 (또는 불법적) 방법을 사용해서 그러한 해독된 통신 내용을 입수할 수 있습니다.

최근에 아랍에미리트연방 정부가 RIM 사에게 모든 블랙베리 통신을 해독할 수 있는 방법을 제공하라고 강요했으나 RIM 사가 거절한 사례가 있습니다. 블랙베리 사용자들은 그들의 정부와 RIM 사 간에 어떤 뉴스나 협상이 있는지 지켜봐야 합니다. 또한, 블랙베리 사용자들은 다른 조직이나 단체가 암호화된 블랙베리 통신을 해독하려고 하는지도 눈여겨 지켜봐야 합니다. 2009 년에 아랍에미리트연방의 최대 통신사인 Etisalat 사는 블랙베리 사용자들의 모든 메시지 사본을 그들이 받을 수 있게 하는 비공식적인 소위 "업데이트"를 블랙베리 유저들에게 보낸 사건이 있었습니다. RIM 사는 곧 블랙베리 유저들에게 그 위장 소프트웨어를 제거하는 업데이트를 보내기는 했지만 블랙베리 유저들은 RIM 사가 직접 보내지 않는 업데이트는 일단 설치하지 않도록 저희들은 권고합니다.

추가적 정보:
Tactical Tech 가 출판한 Mobiles in a Box (영어판)
MobileActive 가 출판한 Mobile Security Risks Primer (영어판)

기타 사항:

블로깅:
블로깅을 시작하는 방법은 다음과 같습니다. 블로깅을 할때 중요한 것은 귀하의 신원을 보호하는 것과 정부가 귀하의 블로그 계정을 차단하더라도 구독자들이 계속해서 귀하의 블로그를 읽을 수 있게 하는 것입니다. 귀하의 사이트의 원래 URL 가 차단되는 경우 다음과 같은 방법을 사용하여 미러 사이트를 설치할 수 있습니다:

Wordpress 및 Tor 를 사용하는 익명 블로깅 (Global Voices 출판)
검열된 Wordpress 블로그를 미러하는 방법 (Global Voices 출판)
안전하게 블로깅하는 방법 (EFF 출판)
블로거의 핸드북 (국경없는 기자회 출판)

동영상을 녹화하는 방법
관련 서적: 변혁을 위한 비디오 및 비디오: 변혁을 위한 비디오를 만드는 방법 – 아랍어 자막 (증인).
인터넷 시큐리티 및 디지털 행동주의를 위한 추가 정보:
Tactical Tech & FrontLine - "Security in a Box": 아랍어 영어
Electronic Frontier Foundation 이 출판한 상세한 안내서: Surveillance Self-Defense 및 축소판 International edition of SSD (둘 다 영어판임).