



사이버 안전에 대한 소개: 온라인을 안전하게 이용하는 방법

인터넷은 우리 삶에서 빼놓을수 없는 일부가 되었으며 생활속에서 많은 것들을 온라인을 통해 할수 있습니다.

보다 안전한 온라인 사용 방법과 개인정보를 보호하는 일반적인 주의사항을 아래와 같이 알려드리려 합니다.

1. 인터넷에서 나 자신을 보호해야합니까?

인터넷에서 사람들은 신원을 쉽게 위조할수 있습니다, 그러므로 귀하의 이메일을 받을 사람, 인터넷 쇼핑시 안전한 사이트인지, 개인정보 및 세부정보를 제공해야하는 상대에 대해 충분히 알 필요가 있습니다.

인터넷 보안 소프트웨어는 사이버 범죄로부터 귀하를 안전하게 보호하는 데 중요한 역할을 합니다.

아래와 같은 몇 가지 상식적인 단계는 사이버 범죄를 어렵게 만듭니다.

- 컴퓨터와 무선 네트워크를 암호로 보호하십시오.
- 낯선 사람에게 개인적으로 타협적인 세부 정보를 제공해서는 안됩니다.
- 보안 소프트웨어 설치하십시오.

2. 인터넷 사용시 직면할수 있는 위험요소들

1) 멀웨어

멀웨어 (악의적인 소프트웨어)는 일반적으로 다른 이해 당사자에게 판매 할 목적으로 컴퓨터를 접속하고 정보를 수집하려는 의도로 만들어집니다.

가장 일반적으로 알려진 멀웨어 유형은 바이러스입니다.

컴퓨터에서 다운로드하여 실행하는 프로그램에 주의해야합니다. 평판이 나쁜 출처에서 프로그램을 다운로드하면 감염되었을 수 있습니다.

안전한 브라우징을 했다고 해도 최신 악성코드나 사용자의 부주의로 인해 악성코드에 감염되는 것을 100% 예방할 수는 없습니다. 따라서 PC 에 백신 소프트웨어를 설치하고 실시간 감시 기능을 활성화해야 합니다.

백신은 인터넷뿐만 아니라 USB, CD 등의 입출력 외장 기기가 검색 되었을 때도 검사를 수행하기 때문에 PC 보안에서는 필수라고 할 수 있습니다.



2) 해커

해커 (또는 봇)는 컴퓨터의 보안 취약성을 악용하여 개인 파일을 접속하려고 시도합니다.

예를 들어, 윈도우 파일 공유에 대해 알고 계십니까? 한 컴퓨터가 네트워크를 통해 다른 컴퓨터로 문서를 보낼때 암호로 보호되어 있지 않은 경우 해커가 이를 탐지하여 파일을 접속하거나 PC 에 바이러스 또는 기타 유형의 악성코드를 이식 할 수 있습니다.

3) 도난, 피싱 및 온라인 신용사기범들을 식별하십시오.

피싱과 온라인 신용 사기범

인터넷상에서는 상호간 말할 수있는 사람에 대한 규칙이 없으므로 사람들은 신용카드 번호 및 은행계좌 번호 / 비밀번호와 같은 개인 정보를 입수하거나 돈을 요구하기 위해 자신이 무언가 또는 다른사람인 것처럼 행동 할 수 있습니다. 본질적으로, 사기범들은 온라인상에서 그럴듯한 비즈니스를 하며 여러분을 이용하려고 합니다. 일반적인 사기는 피싱 시도입니다. 사기범들은 귀하가 알고있는 사람이나 조직으로 가장하여 은행 계좌 세부 정보와 같은 개인 정보를 유출하려합니다.

스팸 및 피싱 사기를 식별하고 인터넷에서 문제가 발생하지 않도록하는 몇 가지 간단한 방법이 있습니다. 다음은 주의해야 할 몇 가지 안전사항입니다.

- 이메일과 발신자의 제목을 확인하십시오. 귀하가 아는 누군가로부터 오는 것이고, 귀하가 등록한 것을 기억하고 있습니까? 그렇지 않은 경우 스팸일 가능성이 큽니다.
- 귀하의 개인 정보를 교환하여 무료로 제공되는 돈이 있습니까? 개인 정보를 보내지 않거나 클릭하거나 링크하지 않으면 부정적 결과가 나올 것이라고 겁을 줍니까? 받는 사람 필드에 귀하의 이름이 있습니까? 이것들은 모두 피싱 사기의 징후입니다.
- 이메일에 철자 및 문법 오류가 있으며 제대로 표시되어 있지 않습니까? '무료'이메일 계정 (outlook.com, yahoo.com, gmail.com)의 이메일입니까? 이러한 표시들이 있고, 발신자 이름이 없다면 의심을 가지고 대처하십시오.

어떤 상품이나 추천에 당첨되었다는 이메일은 매우 매력적일 수 있으며, 많은 사람들이 신뢰를 가집니다. 이런 유형의 이메일을 받는 경우 이름, 주소 및 웹 사이트와 같은 이메일을 받는 이유를 반드시 확인하십시오.



3. 보안 소프트웨어는 무슨 역할을 합니까?

보안 소프트웨어의 유형

좋은 소식은 보안 소프트웨어를 사용하여 대부분의 위협으로부터 자신을 보호 할 수 있다는 것입니다. 컴퓨터에는 기본적인 보안 소프트웨어가 내장되어 있지만 그 위에 소프트웨어를 추가하는것이 더욱더 안전합니다. 보안 소프트웨어에는 아래와 같이 여러 가지 유형이 있습니다.

- 1) **바이러스 백신** : 컴퓨터를 대부분의 유형의 멀웨어로부터 보호하고 나머지는 컴퓨터의 기본 제공 방어 수단으로 사용하는 소프트웨어입니다. 무료 또는 저렴한 가격으로 바이러스 백신 소프트웨어를 얻을 수 있습니다.
- 2) **인터넷 보안 제품군** : 악성 코드, 사기성 이메일, 트릭 웹 사이트, 해커 등 모든 종류의 위협으로부터 컴퓨터를 보호하는 소프트웨어 패키지입니다. 인터넷 보안 스위트에는 연회비 (보통 \$60 ~ \$130)가 있습니다.

컴퓨터 보호하기

- 1) 방화벽은 인터넷 트래픽에 대한 보안 검사점 역할을합니다. 승인된 트래픽 만 통과합니다.
- 2) 바이러스 백신 소프트웨어는 컴퓨터에 들어오는 모든 맬웨어 (바이러스, 스파이웨어 및 애드웨어 포함)를 추적하여 제거합니다. 컴퓨터에는 바이러스 백신 소프트웨어가 제공되지 않으므로 설치해야 합니다.

4. 보안 소프트웨어 선택

PC, 태블릿 또는 스마트 폰과 인터넷에 연결하는 모든 장치는 바이러스 백신 소프트웨어 또는 인터넷 보안 제품군으로 보호하는 것이 안전합니다. 연간 요금을 지불 할 여유가 없으면 무료 바이러스 백신 응용 프로그램을 대신 사용할 수 있습니다. 보안 제품군만큼 시스템을 보호하지는 않지만 기본적인 보호를 제공합니다.

무료 안티 바이러스 프로그램 (바이러스 백신)은 다음과 같습니다

Microsoft: www.microsoft.com/securityessentials

AVG: www.avgfree.com.au

Avast!: www.avast.com

Comodo: www.antivirus.comodo.com



5. 온라인 사용시 자신을 안전하게 지키기 (보안 소프트웨어만으로 충분하지 않음)

컴퓨터에 보안 소프트웨어를 설치하는 것은 온라인에서 자신을 보호하기 위한 크고 중요한 단계입니다. 하지만 보안 소프트웨어만으로 사기범과 사이버 범죄자로부터 전적으로 귀하를 보호할 수는 없습니다. 우리가 온라인으로하는 많은 일에는 중요한 정보 또는 개인 정보가 관련되어 있습니다. 귀하의 개인 정보는 귀하를 식별하는 정보입니다. 귀하의 개인 정보를 보호하기 위해서는 온라인상에서 공개적으로 공유하는 행동에 각별히 주의해야 합니다.

자신을 안전하게 지키기 위해 할 수 있는 몇 가지 간단한 방법이 있습니다.

- 1) 강력하고 독특한 암호 / 암호문을 사용하고 정기적으로 변경하십시오
- 2) 공개 사이트에 개인 정보를 게시하지 마십시오.
- 3) 확실하지 않으면 이메일 첨부 파일을 열지 마십시오.
- 4) 어떤 이메일에 응답하는지 주의하십시오.
- 5) 신용 카드 세부 정보를 누구에게 제공하는지 주의하십시오.
- 6) 신뢰할 수 없는 출처의 프로그램을 설치하지 마십시오.

부인 성명

이 책자 및 동봉 된 자료에 포함 된 정보는 교육 및 정보 제공을 위한 것입니다. 해당 간행물 및 동봉 된 자료는 간행물 및 동봉 된 자료에 언급, 표시 또는 시연 된 제품 또는 서비스의 홍보, 승인 또는 승인을 의미하지 않습니다. 해당 간행물 및 동봉된 자료는 초기 참조 용으로 만 사용됩니다. 포괄적인 안내서이거나 모든 상황에 적용하기 위한 것은 아닙니다. 본 출판물 및 동봉 된 자료에 나오는 정보가 제작 당시에 정확했는지 확인하기 위해 합리적인 노력을 기울였습니다. 그러나 이 간행물의 작성자, 제작자 및 발표자 및 동반 자료 (관련 인물) *는 이 간행물 및 동봉 자료의 정보의 정확성, 신뢰성, 완전성 또는 통화에 대해 어떠한 진술이나 보증도하지 않습니다. 이 간행물에 제공된 정보와 조언 및 동봉 된 자료는 청중이 여기에서 논의 된 문제에 대한 자체 평가를 책임지고 모든 관련 진술, 진술 및 정보를 확인하는 것이 좋습니다. * 해당 인물 : •이 출판물 및 동봉 자료의 정보와 관련하여 모든 명시적 또는 묵시적 보증을 법에서 허용하는 범위 내에서 제외하십시오. •이 간행물 및 동봉 자료의 정보를 업데이트하거나 본 간행물 및 나중에 명시 될 수 있는 동반 자료에 대한 부정확성을 정정 할 의무가 없습니다. • 게시 (및 부수적 인 자료) 및 그 내용 (이 부인 조항의 조건 포함)을 사전 통지없이 언제든지 삭제, 변경 또는 이동할 수 있는 권한을 절대적 재량으로 보유합니다. * 관련자에는 출판물 제작에 관련된 개인, 회사, 파트너십 또는 정부 부서와 해당 임원, 직원 및 대리인이 포함됩니다.

상표 고지



Cyber Safety KOREAN

본 교육 안내서에 언급된 모든 제품명 또는 웹 사이트는 제 3 자의 상표 일 수 있습니다.

지적 재산권 고지 및 면책

저작권 © Telstra Corporation Limited (ABN 33 051 775 556). 판권 소유. Telstra Corporation Limited (ABN 33 051 775 556)의 동의하에 복제된 제 3 자 저작권 및 상표. 이 자료는 호주 법률 및 국제 조약을 통해 저작권법의 보호를받습니다. 이 자료의 어떤 부분도 귀하의 정보, 연구 또는 연구를 제외하고는 전자적, 기계적, 녹음 또는 기타 형식 또는 방법으로 배포, 배포, 복제, 복사, 저장 또는 전송할 수 없습니다.