

Internet Safety

[1] Introduction

우리 모두는 인터넷을 사용할 때 안전해야 한다는 것을 알고 있다. 그렇지만 그것을 어떻게 해야하는지에 대해서는 잘 알지 못한다. 과거에 인터넷 보안이란 대부분이 바이러스로부터 컴퓨터를 보호하는 것이었다. 그러나 오늘날, 인터넷의 막강한 기술적 사회적 영향력으로 인하여 대부분의 이용자들은 identity theft, privacy violations 그리고 harassment(bullying)에 취약해졌다..

이제 여러분이 온라인에서 만날 수 있는 위협의 종류에 대해 알아보기로 하자. 또한 이 강의에서는 여러분 스스로가 자신을 보호하는 방법, 강력한 패스워드를 만드는 방법, 그리고 인터넷을 사용하는데 있어서 여러분의 마음을 안전에 신경 쓰도록 하는 방법에 대해 설명할 것이다.

>안전에 대한 마음을 가짐: Adopting a Safer Mindset

인터넷을 사용할 때 일반적으로 사람들은 실제보다 더 안전하다고 생각한다. 왜 그럴까? 종종 기술의 비인간성은 우리에게 안전에 대한 잘못된 감정을 갖게 하는데, 누구도 컴퓨터 스크린을 통해 우리를 신체적으로 공격할 수 없기 때문이다. 우리는 나에겐 일어나지 않을 것 (it-won't-happen-to-me)이 태도를 갖고 있다. 심지어 우리는 컴퓨터 프로그램들과 그것의 현재 성능이 자동적으로 인터넷 보안에서 우리를 지켜줄 것이라고 믿기도 한다. 때때로 우리는 그것을 이해할 수 없기 때문에 회피하기도 한다. 여러분은 여기에 해당되지 않는가? 다음의 질문에 대해생각해 보자:

- > 당신에 관해 정보를 스스로 검색해 본 적이 있는가?
- > 컴퓨터 보안 프로그램을 설치하고 정기적으로 갱신하는가?
- > 컴퓨터용 외부 백업 소스를 가지고 있는가?
- > 특별할인가라는 이메일이나 광고에 현혹된 적이 있는가?
- > 온라인 쇼핑 시에, 지불페이지에 접속하기 전에 해당 사이트의 보안 상태를 확인하는가?
- > Facebook 등에서 사용하는 social networking accounts가 비밀보호 프로그램에 맞는가?

위의 질문에 신경이 쓰인다고? 걱정하지 마라. 이제 우리는 인터넷을 사용하는 동안 여러분 자신과 컴퓨터를 안전하게 보호하는 방법에 대하여 알아볼 것이다.

>인터넷을 쇼핑물이라 생각하라.

일반적으로 쇼핑물은 위한 장소가아니다. 그곳에서 쇼핑도하고, 사람도 만나고 하지만 주위도 해야 한다. 우리는 주차장에 차 문을 열어 놓고 쇼핑을 하거나 직원이나 낯선 사람에게 비밀번호를 알려 주지 않는다.

인터넷에서도 똑같은 원칙이 적용된다. 우리가 마우스 클릭을 두려워할 필요는 없지만 우리 스스로 안전에 대해서 조심하여야 한다.

>인터넷 위협의 이해: Understanding Internet Threats

우리 자신을 보호하기 앞서서 먼저 인터넷의 위협에 대하여 이해하여야 한다.



<Pharming>

파밍은 사용자의 개인 정보에 액세스하기 위해 합법적인 웹 사이트의 트래픽을 다른 불법 웹 사이트로 리디렉션하는 데 사용되는 기술입니다.

<Phishing>

피싱은 합법적인 웹 사이트의 공식 커뮤니케이션처럼 위장한 메일 또는 인스턴트 메시징 scam(사기)입니다. 사용자를 속여 암호, 신용 카드 세부 정보 등과 같은 민감한 정보를 제공합니다.

<Spyware>

스파이웨어는 사용자가 모르는 사이에 사용자에게 대한 정보를 수집하고 종종 검색 습관을 추적하고 팝업 광고를 만드는 맬웨어 유형입니다. 개인 정보를 침해하는 것과 함께 때때로 컴퓨터의 기능을 방해 할 수 있습니다.

스파이웨어는 때때로 다른 소프트웨어와 함께 제공됩니다. 소프트웨어를 다운로드하기 전에 리뷰를 읽고 평판이 좋은지 확인하는 것이 좋습니다.

<Browser Hijacking>

브라우저 하이재킹은 맬웨어나 스파이웨어가 특정 웹 사이트에 더 많은 히트를 치기 위해 브라우저의 홈페이지를 자체적으로 대체할 때 발생합니다.

<Clickjacking>

클릭 재킹은 합법적인 웹 페이지로 보이는 투명 레이어에 링크를 추가하여 사용자가 악성

링크를 클릭하도록 속이는 기술입니다.

사용자는 합법적 인 페이지에서 버튼이나 링크를 클릭한다고 생각하지만 실제로는 숨겨진 페이지에서 숨겨진 링크를 클릭하고 프로세스에서 기밀 정보에 대한 액세스를 제공하는 경우가 많습니다.

<Hoax>

혹스는 임박한 바이러스에 대해 경고하여 사용자가 혹스 이메일을 계속해서 전달하도록 위협하는 이메일 체인 편지(email chain letter)입니다.

<Mousertrapping>

마우스 트래핑은 방문자를 윈도우에 locking하거나, 바탕 화면에서 여러 창을 열거나, 닫을 수 없는 윈도우에 자신들의 웹 사이트를 다시 시작하도록 하여 웹 사이트를 떠나지 못하게 합니다.

>인터넷 보안과 프라이버시: Internet Safety and Privacy

과거에 인터넷 안전은 일반적으로 컴퓨터 하드웨어에 대한 위협이나 신원 도용을 의미했지만 이제는 인터넷이 점점 더 사회적으로 변하면서 사생활 보호 (사생활 보호)가 중요한 안전 문제가 되었습니다. 개인 정보 침해는 특히 우리의 정신적, 육체적 안녕에 영향을 미치므로 다음과 같은 이유로 고통이나 피해를 입힐 수 있습니다:

- > Undesired advertisements that can be annoying
- > Embarrassing or humiliating photos or videos
- > Legal entanglements(연루) from libelous(명예훼손) posts
- > Cyber-harassment or cyber-stalking
- > Identity theft
- > Offline or “real world“ crimes

>전문용어의 이해: Understanding the lingo



〈Sockpuppet〉

sockpuppet(양말 인형)은 누군가가 어떤 종류의 개인적인 이득을 위해 다른 사람을 속이기 위해 만들고 사용하는 가짜 신원입니다. 대부분의 웹 사이트에서는 둘 이상의 계정을 가질 수 있으므로 양말 인형을 쉽게 만들 수 있습니다.

예를 들어 John은 동일한 채팅 서비스에 대해 John45, Sarah03 및 HarmonicasRock12와 같은 몇 가지 온라인 ID를 가질 수 있습니다. 그가 HarmonicasRock12 일 때, 그는 30 세의 음악 애호가인 척하여 어떤 음악 상점에 가는지 알 수 있습니다. 그리고 그가 Sarah03 일 때, 그는 당신이 대학에 진학한 곳을 알아내기 위해 20세 대학생인 척 할 수 있습니다.

〈Avatar〉

아바타는 자신을 가상으로 표현한 것입니다. 이 용어는 일반적으로 가상 이미지를 나타냅니다. 소셜 네트워킹 프로필에서 사진을 사용하는 대신 아바타를 사용하여 개인정보를 보호할 수 있습니다.

〈Dooced〉

누군가가 블로그 나 소셜 네트워킹 사이트에 게시한 내용 때문에 직장을 잃는다면 그들은 파멸(dooced) 된 것입니다.

〈Troll〉

트롤은 사람들을 흥분하고 산만하게 하기 위해 댓글을 게시하는 사람입니다. 트롤은 무례한 말을 하거나 잘못된 정보를 주장하거나 당면한 주제와 관련없는 질문을 하기도 합니다. 명백한 트롤링 게시물에 응답하는 사람들은 트롤에게 먹이를 주는 것입니다. 이로 인해 종종 트롤이 돌아와 토론을 계속 방해하게하는 원인이 됩니다.

〈Flame war〉

Flame war(화염 전쟁)은 웹 포럼, 메일링 리스트 또는 채팅방과 같은 소셜 미디어 매체에서 열린 논쟁을 유도함으로써, 의도적으로 모욕적인 댓글과 인신 공격이 대화의 초점이 됩니다.

<Screen name>

사용자 이름이라고도 하는 화면 이름은 소셜 미디어가 구성 요소인 웹 사이트의 사용자를 식별하는 데 사용되는 가상 이름입니다. 대화명은 실명 또는 가명일 수 있습니다.

낯선 사람과 정기적으로 교류하는 사이트에서는 가명을 선택하는 것이 좋습니다. tennis247 또는 partyboy18과 같은 이해할 수 있는 가명을 선택할 때 그것은 속을 수 있는 이미지이거나 유혹하려는 응답에 조심하여야 합니다.

<Flamebait>

누군가가 화를 내도록 하거나 화를 부르는 응답을 올리는 댓글을 플레임 베이트 (flamebait) 라고 합니다. 누군가가 이런 댓글에 응답하면 미끼를 물었다(taken the bait)고 합니다.

<Meme>

Meme은 캐치 프레이즈, 속임수, 주제, 개념 또는 미디어와 같이 바이러스 처럼 퍼지거나 인터넷을 통해 빠르게 확산된 어떤 것입니다.

미미는 종종 귀엽거나, 재미있거나, 호기심이 많아서 전달하고 싶게 만듭니다! 이메일을 전달하는 경우 나중에 해당 이메일을 받는 모든 사람이 귀하의 이메일 주소에 액세스할 수 있다는 점을 기억하십시오.

<Posts>

사람들이 블로그, 뉴스 그룹 및 포럼과 같은 소셜 미디어와 관련된 웹 사이트에 게시하는 콘텐츠를 posts(게시물)이라고합니다. Twitter는 사용자가 Twitter 사이트에 작성한 posts를 트윗(tweets)이라고합니다.

포스트는 사이트에 액세스할 수 있는 모든 사람이 사용할 수 있습니다. 게시된 포스트를 변경하거나 삭제할 수 있는 옵션이 항상 여러분에게 있는 것은 아닙니다. 귀하 또는 귀하의 온라인 신원을 즉시 공개적으로 표현되므로, 포스트하기 전에 숙고하세요!

>자신을 구글하라: Googling Yourself

간단한 웹 검색만으로 얼마나 빨리 당신과 당신의 배경에 대해 알아낼 수 있는지 알고 계십니까? 대부분의 사람들은 주소, 전화 번호, 때로는 사진과 같은 개인 기록을 온라인에서 누구나 쉽게 액세스 할 수 있다는 사실을 모릅니다. 이 정보는 유해하지 않을 수 있지만 어떤 상황에서는 무엇이 있는지 알지 못해 위험에 처할 수 있습니다. 예를 들어, 누군가 집 전화 번호 만 알아 내면 간단한 온라인 검색만으로 집 주소와 경로를 찾을 수 있습니다. 정기적으로 Google을 검색하여 어떤 웹 사이트와 공개 데이터베이스가 귀하에 대한 정보를 공유하는지 알아보십시오.

>탐색을 통해 최대한 얻도록 하라: Make the Most out of Your Search

가장 정확하고 완전한 결과를 얻으려면 이름, 이메일 주소, 집과 직장 주소, 전화 번호와 같은 검색어를 다양한 방법으로 입력하세요. 또한 검색어 주위에 따옴표를 넣으면 검색

엔진이 사용자가 작성한 방식 그대로 특정 구문을 찾도록 지시합니다. 이것은 당신의 검색을 더 효율적으로 만들 것입니다

- > First name and last name: “Will Bolding”
- > First, middle, and last name: “Will Edward Bolding”
- > Last name followed by a comma and then your first name: “Bolding, Will”
- > Last name followed by a comma, your first name and middle name: “Bolding, Will Edward”
- > Street address: “2521 Street Address Lane”
- > Phone number (using no spaces or hyphens searches all instances of your number): “9195554444”
- > Email address: “boldingsoccer@email.com”

>웹사이트에서 자신의 정보를 제거하라: Removing Your Information from Websites

웹 사이트에 정보 삭제를 요청할 수 있습니다. 그들이 항상 귀하의 요청을 준수 할 의무가 있는 것은 아닙니다. 귀하에 대해 게시된 정보가 귀하의 안전에 직접적인 위협이되고 콘텐츠를 제거하기 위해 웹 사이트와 협상하는 데 도움이 필요한 경우 WiredSafety.org에 문의할 수 있습니다. 그들은 귀하의 특정 사례에 대해 조언 할 수 있습니다.

Reputation.com과 같은 외부 서비스에 유료로 온라인에서 개인 정보를 제거할 수도 있습니다. 대부분의 사람들에게 이런 종류의 서비스는 필요하지 않지만 선택 사항이라는 점을 명심하십시오.

[2] Passwords: The First Step to Safety

>패스워드: 보안을 위한 첫 번째 조치: Passwords: The First Step to Safety

대부분의 사람들은 암호를 만드는 데 많은 생각을 하지 않습니다. 일반적으로 짧고 기억하기 쉬운 비밀번호를 생성하거나 보유한 모든 계정에 동일한 비밀번호를 사용하는 것이 가장 쉽습니다. 결국 일반 사람들은 아마 당신의 암호를 추측할 수 없을 것입니다.

그러나 해커는 올바른 암호를 찾을 때까지 다양한 암호를 계속 테스트할 수 있는 암호 해독 소프트웨어를 자주 사용하고 취약한 암호를 쉽게 해독할 수 있습니다. 강력한 암호를 만들면 개인 정보 나 금융 정보가 도난 당할 가능성을 크게 줄일 수 있습니다.

>일반적인 패스워드의 실수Common Password Mistakes

많은 사람들이 배우자의 이름, 취미 또는 단순한 패턴을 기반으로 암호를 만듭니다. 이러한 유형의 암호는 기억하기 쉽기 때문입니다. 불행히도 해커가 추측하기가 매우 쉽습니다. 강

력한 암호를 만들려면 이러한 유형의 일반적인 실수를 피해야 합니다.

>강력한 패스워드를 만드는 팁: Tips For Creating Strong Passwords:

- **결코 대인정보를 사용하지 마라:**

이름, 생일 또는 배우자의 이름과 같은 개인 정보를 사용하지 마십시오. 개인 정보는 종종 공개적으로 사용 가능하므로 다른 사람이 암호를 추측하기가 훨씬 쉽습니다.

- **보다 긴 패스워드를 사용하라: Use a longer password.**

비밀번호는 6자 이상이어야 하며 추가 보안을 위해 12자 이상이어야 합니다 (사이트에서 허용하는 경우). 암호를 적어 두어야 하는 경우 안전한 장소에 보관하십시오. 암호를 “암호화”하거나 다른 사람이 이해할 수 없는 힌트를 적어 두는 것이 더 좋습니다.

- **각 계정마다 동일한 패스워드를 사용하지 마라: Don't use the same password for each account.**

누군가가 한 계정의 비밀번호를 발견하면 다른 모든 계정이 취약해 집니다. 숫자, 기호 및 대문자와 소문자를 모두 포함하십시오 (사이트에서 허용하는 경우). 사전에서 찾을 수 있는 단어를 사용하지 마십시오. 예를 들어 “swimming1”은 매우 약한 패스워드입니다.

암호.

- **무작위 패스워드가 가장 강력하다: Random passwords are the strongest.**

자신의 생각을 시도하는 대신 암호 생성기를 사용하십시오. 임의의 암호는 기억하기가 더 어렵기 때문에 니모닉(mnemonic) 장치를 만드십시오. 예를 들어, “H = jNp2 #”는 “HARRY = jessica NOKIA paris 2 #”로 기억 될 수 있습니다. 이것은 여전히 무작위로 보일 수 있지만 약간의 연습을 통해 비교적 쉽게 암기할 수 있습니다.

- **패스워드 매니저 사용하기: Using Password Managers.**

다른 사람이 쉽게 볼 수 있도록 종이에 암호를 작성하는 대신 암호 관리기를 사용하여 온라인으로 암호화하고 저장할 수 있습니다. 일부 암호 관리기는 임의의 암호를 생성하여 정보를 더욱 안전하게 만들 수 있습니다. 비밀번호 관리기의 예로는 LastPass, KeePass, Firefox의 비밀번호 관리자 및 Google Chrome의 비밀번호 관리기가 있습니다.

[3] Protecting Your Computer from Internet Threats

바이러스, 트로이 목마, 웜 및 스파이웨어는 모두 컴퓨터 시스템을 손상시킬 수 있는 위협입니다. 컴퓨터를 보호해야 한다는 것을 알고 있지만 시중에 나와있는 바이러스 백신 프로그램이 너무 많기 때문에 특정 요구 사항에 가장 적합한 것이 무엇인지 어떻게 알 수 있을

까요?

이 레슨에서는 어떤 종류의 바이러스 백신(antivirus)이 필요한지, 어떤 제품이 가장 적합한지를 결정할 수 있는 방법을 살펴 봅니다. 또한 시스템을 백업하고 보안 프로그램을 최대한 활용하는 방법에 대해 설명합니다.

>어떤 보호가 필요한가: What Protection Do You Need?

인터넷 위협에 대한 최선의 방어는 좋은 바이러스 백신 소프트웨어 또는 때때로 알려진 맬웨어 방지 소프트웨어입니다. 바이러스 백신 소프트웨어는 감염된 이메일 첨부 파일, 손상된 웹 사이트, 인터넷 웹, 스파이웨어 등으로부터 사용자를 보호할 수 있습니다. 시장에는 수 많은 바이러스 백신 제품이 있으므로 필요한 것을 파악하는 것은 매우 혼란스러울 수 있습니다. 따라서 바이러스 백신 프로그램에서 무엇을 찾아야 하는지에 대한 더 나은 아이디어를 제공하기 위해 고려해야 할 사항을 간략하게 설명합니다.

>복수의 보호: Multiple Protections

여러분이 얻을 수 있는 보호에는 다음 세 가지 구성 요소가 포함되어야 합니다:

- **안티 바이러스** - 특히 바이러스로부터 보호합니다.
- **안티 스파이웨어** - 사용자 당신이 모르는 정보를 수집할 수 있는 악성 소프트웨어로부터 보호합니다.
- **방화벽**-인터넷을 통해 컴퓨터에 도달하려는 위협을 차단합니다.

일부 보안 제품군은 많은 추가 보호 기능을 제공하지만, 위의 3 가지는 주요 구성 요소입니다.

>보안 스위트: Security Suites

대부분의 바이러스 백신 회사는 바이러스만 검사하는 독립 실행형 제품과 방화벽, 스팸 필터링, 스파이웨어 방지 도구 등과 같은 추가 보호 기능을 제공하는 패키지 보안 제품군을 모두 제공합니다.

■ 보안 스위트 : Security Suites.

보안 제품군은 일반적으로 관리하기가 더 쉽고 초보자에게 유용 할 수있는 광범위한 보호 기능을 제공합니다. 그러나 어떤 경우에는 제품군의 추가 기능이 해당 기능에 대한 독립형 제품만큼 좋지 않습니다. 또한 일부 제품군은 컴퓨터 속도를 늦추는 경향이 있습니다.

■ 독립 제품 : 독립형 제품: Stand-Alone Products

고급 사용자는 때로 선택 및 혼합 방식을 선호하여 각 구성 요소에 가장 적합한 제품을 조사 및 선택하여 자체 보안 시스템을 구축합니다.

>구입전 고려해야 할 사항: Things to Consider Before You Buy

■ 컴퓨터를 조사하라: Investigate Your Computer

새 컴퓨터를 구입하는 경우 이미 제공되는 보호 유형에 대해 영업 담당자에게 문의해야 합니다. 일부 컴퓨터에는 보안 소프트웨어가 함께 제공되지만 AS 기간 후에 구입해야 할 수도 있습니다.

또한 웹 브라우저에는 검토해야 하는 보안 설정이 있습니다. 새로운 바이러스 백신 소프트웨어를 선택하기 전에 컴퓨터에 이미 어떤 보호 기능이 있는지 완전히 조사하는 것이

■ 무료 대 유료 프리미엄 소프트웨어: Free vs. Paid Premium Software

적절한 수준의 보호를 제공 할 수 있는 많은 무료 바이러스 백신 프로그램이 있습니다. 그러나 많은 무료 바이러스 백신은 기업이 결국 업그레이드하기를 바라는 유료 소프트웨어 프로그램의 축소 버전입니다. 무료 바이러스 백신의 단점은 종종 기술 지원이 포함되지 않고 기능과 업데이트 기능이 제한될 수 있다는 것입니다. 대부분의 유료 소프트웨어는 최신 소프트웨어 및 업데이트를 받으려면 갱신이 필요한 연간 구독을 기반으로 합니다.

■ 맥 유저: Mac Users

전통적으로 Mac 바이러스가 적기 때문에 많은 Mac 사용자가 바이러스 백신 소프트웨어를 사용하지 않습니다. 그러나 최근에 Mac 바이러스가 더 보편화되었습니다. 이제 많은 전문가들이 바이러스 백신 소프트웨어를 사용하고 OS X 방화벽을 사용하는 것을 권장합니다.

■ 공포웨어: Scareware

보안 경고로 위장한 악성 링크는 사이버 범죄자들에게 인기있는 전술이 되었습니다. 이러한 공식적인 통지는 컴퓨터에 바이러스가 있음을 경고하고 링크를 클릭하거나 프로그램을 다운로드하여 해결해야 한다고 주장합니다. 링크를 클릭하도록 겁을 주려고 하지만 실제로는 링크가 악성 코드로 이어집니다.

이러한 유형의 사기에 대한 단어는 scareware입니다. Scareware는 바이러스 백신 소프트웨어에 대한 많은 광고에도 표시되므로 이 소프트웨어를 검색하기 시작할 때 주소 도메인을 확인하고 조사를 위해 합법적인 웹 사이트로 이동하는지 확인하십시오. 웹 브라우저 나 이메일을 통해 표시되는 모든 바이러스 경고는 가짜(bogus)입니다.

>엔타이바이러스 소프트웨어의 선택 방법: How to Choose an Antivirus Software

이제 요구 사항을 평가하고 독립 실행형 제품 또는 보안 제품군을 원하는지를 결정했으므로 바이러스 백신 소프트웨어를 선택하는 프로세스를 시작할 수 있습니다. 조사에서 중점을 두어야 할 사항에 대해 알아보려면 아래의 대화식을 검토하십시오.

■ 엔타이바이러스 소프트웨어 사용의 전략: Strategies for Using an Antivirus Software

기억해야 할 가장 중요한 것은 새로운 바이러스가 지속적으로 도입되고 있다는 것입니다.

따라서 바이러스 백신 소프트웨어는 최신 업데이트만큼만 우수합니다. 바이러스 백신 소프트웨어를 효과적으로 사용하려면 다음 전략을 따르십시오.

- 자동 업데이트 기능이 켜져 있는지 확인하십시오.
- 갱신 통지를 무시하지 마십시오. 구독이 만료되면 업데이트 수신이 중단됩니다.
- 특정 프로그램, 업그레이드 또는 다운로드를 허용하기 위해 바이러스 백신을 비활성화해야 하는 경우가 있습니다. 완료되면 프로그램을 다시 활성화하는 것을 잊지 마십시오.
- 바이러스 백신은 어려운 문제를 처리하기 위한 구체적인 지침을 제공해야 하지만 문제가 있는 경우 기술 지원에 문의하십시오.
- 바이러스 백신 프로그램이 마음에 들지 않으면 새 제품을 설치하기 전에 제거했는지 확인하십시오.

■ **고려해야 할 추가적 컴퓨터 보안 조치들: Additional Computer Safety Practices to Consider**
다음은 컴퓨터를 건강하게 유지하는 데 사용할 수 있는 몇 가지 추가 정보입니다.

• 정기적으로 컴퓨터

우리 중 일부는 항상 컴퓨터를 켜두지만 적어도 일주일에 한 번 컴퓨터를 끄고 다시 시작하는 것이 좋습니다. 이렇게 하면 컴퓨터가 정기적인 진단 검사를 수행하고 문제가 되기 전에 사소한 문제를 해결할 수 있습니다.

• 소프트웨어 업데이트 설치

운영 체제에서 소프트웨어 업데이트를 알리면 다운로드하여 설치하십시오. 소프트웨어 업데이트는 운영 체제의 보안 취약성 및 기타 버그를 수정하도록 설계되었습니다. 이렇게 하면 최신 위협으로부터 컴퓨터를 보호하는 데 도움이 됩니다.

• 시스템 복원 사용

문제를 일으키는 다운로드가 있는 경우 운영 체제의 시스템 복원 기능을 사용해보십시오. 이 기능을 사용하면 문제가 발생하기 전의 시간과 장소로 컴퓨터를 복원할 수 있습니다.

>컴퓨터 백업: Back Up Your Computer

바이러스 백신 보호 기능을 사용하면 악성 코드로 인해 파일을 잃을 가능성이 크게 줄어듭니다. 그러나 100% 보안을 제공하는 제품은 없습니다. 따라서 외부 소스에 파일을 백업하는 것이 좋습니다. Windows 및 Mac 운영 체제에는 내부 백업 시스템이 함께 제공되지만 컴퓨터를 분실, 손상 또는 도난당한 경우 도움이되지 않습니다. 파일을 외부에서 백업하는 경우가정용 사용자를 위한 두 가지 기본 옵션, 외부 하드 드라이브 또는 온라인 백업 서비스가 있습니다.

>외장 하드 드라이브: External Hard Drives

외장 하드 드라이브를 구입하여 컴퓨터의 내용을 복사 할 수 있습니다. 초기 백업에는 몇 시간이 걸릴 수 있으므로 컴퓨터를 액세스할 필요가 없는 시간을 선택해야 합니다. 일반적으로 밤새 백업을 실행하는 것이 가장 좋습니다. 후속 백업은 정기적으로 수행해야 하지만 드라이브는 최신 파일만 복사하면 되므로 오래 걸리지 않습니다.

Western Digital, Iomega 및 Seagate는 널리 사용되는 외장 하드 드라이브를 생산합니다. 스토리지 요구 사항에 가장 적합한 제품을 조사하거나 컴퓨터 영업 담당자에게 권장 사항을 요청하십시오.

온라인 백업 서비스와 비교할 때 한 가지 단점은 컴퓨터와 마찬가지로 외장 하드 드라이브가 분실, 손상 또는 도난 당할 수 있다는 것입니다. 따라서 사용하지 않을 때는 드라이브를 안전한 장소에 보관하는 것이 중요합니다.

>온라인 백업 서비스 및 클라우드: Online Backup Services and the Cloud

파일을 온라인 즉, 클라우드에 백업할 수도 있습니다. 클라우드에 무언가를 저장하면 컴퓨터가 분실, 손상 또는 도난당하는 것을 방지할 수 있습니다.

이 기술을 활용하는 인기있는 온라인 백업 서비스에는 Mozy, Carbonite 및 Box가 있습니다. 이러한 사이트에서 제공하는 저장 공간의 양은 다양하며 적절한 저장을 위해 월별 또는 연간 요금을 지불해야 할 수 있습니다. 다시 말하지만, 이러한 서비스는 지속적으로 변화하고 다양한 기능을 제공하므로 조사를 늘 하여야 합니다..

온라인 백업 서비스의 한 가지 단점은 초기 백업이 느릴 수 있으며 많은 양의 파일이 있는 경우 업로드하는 데 며칠이 걸릴 수도 있다는 것입니다. 그러나 후속 백업은 오래 걸리지 않습니다.

[4] Email Tips for Scams and Spam

이메일은 의사 소통을 위한 필수 도구가 되었으며, 이것이 scammers(사기꾼), 사이버 범죄자 및 광고 회사들에게 인기있는 이유입니다. 피싱 사기 및 맬웨어로부터 자신을 보호하려면 메일을 안전하게 관리하는 방법을 배우는 것이 중요합니다.

이 레슨에서는 스팸 및 이메일 첨부 파일을 관리하기 위한 팁을 학습합니다. 또한 피싱 사기를 식별하고 방지하는 방법을 배웁니다.

>Spam

스팸은 정크 메일 또는 원치 않는 이메일 광고의 또 다른 용어입니다. 오늘날 대부분의 이메일은 스팸입니다. 스팸머가 수천 명의 사람들에게 동시에 이메일을 보내는 것은 매우 쉽고 저렴하며 익명으로 할 수 있어 스팸 방지법을 시행하기 어렵습니다. 피싱 사기 및 멀웨어

어는 스팸에 포함되는 경우가 많으므로 편지함에서 받은 스팸을 효과적으로 관리 할 수 있어야 합니다.

>스팸을 다루는 팁: Tips For Dealing With Spam:

• 스팸 블로커를 사용하라: Use a Spam Blocker.

스팸 차단기는 받은 편지함에 들어가는 스팸의 양을 크게 줄일 수 있습니다. Yahoo 또는 Gmail과 같은 대부분의 온라인 이메일 서비스에는 스팸 차단 기능이 내장되어 있습니다. Outlook 또는 다른 이메일 프로그램과 함께 사용할 수 있는 MailWasher와 같은 별도의 스팸 방지 프로그램을 사용할 수도 있습니다. 안타깝게도 스팸 차단기를 사용해도 일부 스팸은 통과할 수 있습니다.

• 스팸에 대응하지 마라: Don't Reply to Spam.

스팸 이메일에 답장하거나 이메일에 있는 링크를 클릭하여 구독을 취소하고 싶을 수 있습니다. 이것은 귀하가 구독한 합법적인 이메일에서 할 수 있습니다. 그러나 스팸 발송자는 이러한 요청을 거의 받아들이지 않습니다. 실제로 회신하거나 링크를 클릭하면 스팸 발송자에게 이메일 주소가 기능하는 것을 확인하게 되어 결국 더 많은 스팸을 받게 될 수 있습니다.

• 이미지를 꺼라: Turn Off Images.

이메일에는 스팸 발송자가 추적 할 수있는 이미지가 포함될 수 있습니다. 이메일을 열면 이미지가 로드되고 스팸머가 이메일 주소가 작동한다는 것을 알 수 있어 더 많은 스팸이 보낼 수 있습니다.

• 미리보기 화면을 꺼라: Turn Off Your Preview Pane

(이메일 서비스가 한 개인 경우). 전자 메일이 미리보기 창에 자동으로 표시될 때 스팸을 보지 않도록 할 수 없습니다. 스팸 메시지를 보면 실제로 더 많은 스팸을 받을 수 있습니다. 따라서 스팸을 방지하려는 욕구와 함께 미리보기 창 사용의 편리함을 평가해야 합니다.

• 스팸 폴더를 주기적으로 체크하라: Regularly Check Your Spam Folder.

때때로 스팸 차단기는 합법적인 이메일도 차단합니다. 스팸 폴더를 정기적으로 확인하여 중요한 이메일이 누락되지 않았는지 확인하는 것이 좋습니다. 차단되는 합법적인 이메일을 “허용”하는 설정에 대해 이메일 프로그램에서 확인하십시오.

>Email Scams

많은 스팸 이메일은 귀하에게 무언가를 판매하려는 것이 아니라 귀하의 돈이나 개인 정보를 훔치려고 합니다. 이메일 scams(사기)는 다양한 형태로 제공되지만 일반적으로 너무 좋은 것을 약속하거나, 행동하지 않으면 나쁜 일이 발생할 것이라고 생각하게 만드는 방식으로 작동합니다. 인기있는 이메일 사기에는 재택 근무 제안, 체중 감량 요청, 부채 구제 프로그램 및 만병통치 제품 등이 포함됩니다.

>Advance-Fee Fraud

일정 금액의 돈을 벌면 무언가를 약속하는 이메일이나 분류 광고를 본 적이 있습니까? 이러한 것에 대한 단어는 **Advance-Fee Fraud**(선불 사기)입니다. 실제 사람 (거의 항상 거짓인 “개인 이야기”를 공유하여 사용자를 속이거나 오도하려는 사람)과 대응하기 때문에 다른 이메일 사기와는 다릅니다.

선불 사기의 가장 악명 높은 예 중 하나는 Nigerian letter scam(나이지리아 편지 사기)입니다.

>Phishing

피싱은 개인 정보를 전달하도록 속이기 위해 이메일이 은행이나 다른 신뢰할 수 있는 출처에서 온 것처럼 가장하는 사기 유형입니다. 사기꾼은 이 정보를 사용하여 은행 계좌에서 돈을 인출하거나 신원을 도용할 수 있습니다. 피싱 이메일은 종종 긴박감을 느끼게 합니다. 예를 들어 신용 카드에 “승인되지 않은 청구”가 발생했으며 귀하의 정보를 즉시 확인해야 한다고 주장할 수 있습니다.

>추가 팁: Additional Tips and Resources

• 링크를 따라가지 마라: Don't follow the link.

“공식적인” 것처럼 보이기 위해 합법적인 회사의 로고를 이메일이 사용하는 것은 쉽지만, 클릭하는 링크는 그늘진(shady) 사이트로 연결될 수 있습니다. 항상 웹 주소를 입력하거나 자신의 북마크 중 하나를 클릭하여 은행 또는 기타 신뢰할 수 있는 웹 사이트로 이동하십시오.

• 스캠과 스팸을 보고하라: Report scams and spam.

일부 이메일 서비스 제공업체에는 “이것은 스팸입니다” 버튼 또는 스팸을 신고하는 다른 방법이 있습니다. 허위 사실을 당한 회사에 연락하여 스팸을 신고할 수도 있습니다. 또 다른 옵션은 spam@uce.gov로 연방 거래위원회 (Federal Trade Commission)에 스팸 보고서를 이메일로 보내는 것입니다.

• 더 많은 정보를 얻어라: Get more information

FBI.gov의 새로운 이메일 사기 및 경고 사이트를 방문하고 OnGuardOnline.gov의 피싱을 방문하여 특정 사기에 대해 알아보십시오.

>이메일 첨가물 다루기: Dealing with Email Attachments

이메일 첨부 파일은 바이러스 및 기타 맬웨어를 포함할 수 있기 때문에 특히 위험합니다. 첨부 파일을 열면 맬웨어가 컴퓨터에 자동으로 설치될 수 있으며 아무 일도 일어나지 않았다는 사실조차 깨닫지 못할 수도 있습니다. 맬웨어는 컴퓨터의 파일을 손상시키거나 암호를

훔치거나 스파이를 할 수 있으므로 첨부 파일을 받을 때 특히 주의해야 합니다.

>첨가물 다룰 때의 팁: Tips For Dealing With Attachments:

- 원치 않는 첨가물은 열지 마라: Don't open any attachment that you weren't expecting.

아는 사람이 보낸 이메일처럼 보이더라도 바이러스에 의해 자동으로 전송되었을 수 있습니다. 그것은 많은 이메일 바이러스를 퍼지게 하는 것 입니다. 친구로부터 첨부 파일을 받으면 해당 친구에게 전화 나 이메일로 보냈는지를 확인해야 합니다.

- 엔타이바이러스 소프트웨어를 갱신하라: Keep your antivirus software updated.

바이러스는 빠르게 확산 될 수 있으며 바이러스 백신 소프트웨어가 최신 상태가 아니면 새로운 바이러스를 차단하지 못할 수 있습니다.

- 컴퓨터의 파이어월을 가동시켜라: Keep your computer's firewall on.

방화벽 소프트웨어는 사람이나 맬웨어가 인터넷을 통해 컴퓨터에 액세스하는 것을 방지합니다.

- 다운로드 전에 바이러스용 첨가물 리스트를 스캔하라: Scan attachments for viruses before downloading.

많은 온라인 이메일 제공 업체는 첨부 파일에서 바이러스를 검색할 수 있으며, 일부는 첨부 파일을 검색하지 않고는 다운로드 할 수 없습니다.

[5] Protecting Your Financial Transactions

인터넷은 बैं킹, 쇼핑 및 기타 금융 거래를 온라인으로 매우 편리하게 만들었습니다. 그러나 우리의 돈에 관해서는 우리의 거래가 안전한지 확인하고 싶습니다.

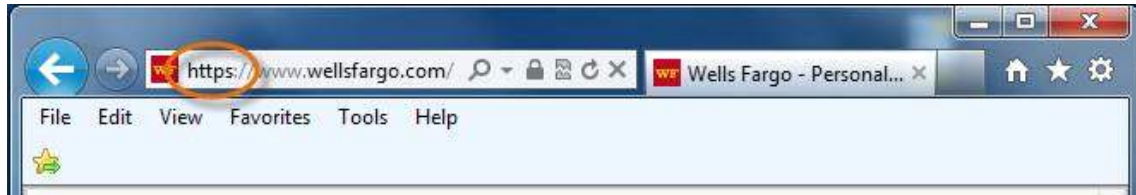
이 강의에서는 돈과 인터넷을 다룰 때 채택해야 할 전략을 검토합니다. SSL 보안 인증서 확인을 포함하여 웹 사이트가 안전한지 확인하는 방법을 배웁니다. 또한 온라인 쇼핑을 안전하고 즐거운 경험으로 만들기 위해 취해야 할 조치를 알려드립니다.

>금융거래 시, 웹 사이트 보안이 필요할 때:When is a Website Secure for Financial Transactions?

민감한 정보 나 금융 정보를 온라인으로 보내기 전에 보안 사이트와 통신하고 있는지 알아야 합니다. 보안 사이트는 전송하는 모든 정보가 암호화되었는지, 인터넷을 통해 이동할 때 보호되는지를 확인합니다. https 주소 제목과 브라우저의 보안 기호는 보안 사이트에 있음을 알려주는 두 가지 표시입니다.

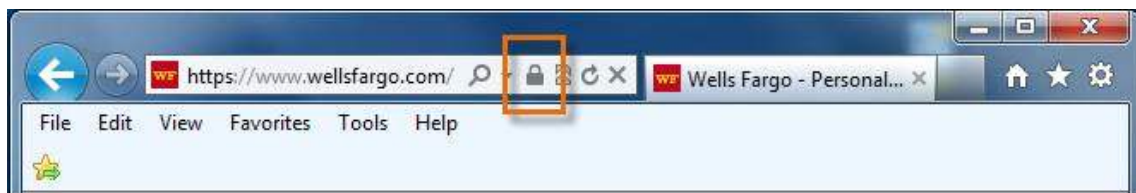
>>Https

웹 주소는 http 또는 https로 시작합니다. 주소가 https 인 경우 보내는 정보가 암호화되어 사이버 범죄자가 가로채면 의미없는 말(gibberish)처럼 보입니다



>>Security Symbol

브라우저는 보안 기호 또는 자물쇠를 사용하여 브라우저가 웹 사이트가 안전한 사이트인지 확인함을 나타냅니다. 아래 예에서 볼 수 있듯이 각 브라우저의 기호 모양은 약간 다를 수 있으며 일반적으로 주소 표시 줄에 있습니다.



>보안 경고 및 SSL 인증: Security Alerts and the SSL Certificate

>>SSL Certificate

보안 사이트에는 SSL(Secure Sockets Layer) 인증서가 있습니다. SSL 인증서는 두 가지 작업을 수행합니다. 첫째, 가상 여권이나 운전 면허증과 같은 역할을 합니다. 그것은 “나는 내가 나라고 말하는 사람이다(I am who I say I am).”라는 뜻입니다. 둘째, 암호화가 가능합니다. 사이트에 SSL 인증서가 없는 경우 주소는 https 대신 http로 시작하고 브라우저에 잠금 기호가 표시되지 않습니다. SSL 인증서가 있는 경우 브라우저 잠금을 두 번 클릭하여 액세스할 수 있습니다.

>>Security Alerts

현재 버전의 Internet Explorer, Firefox 및 Chrome은 SSL 인증서를 확인합니다. 인증서가 최신 상태가 아니거나 신뢰할 수 있는 인증 기관에서 발급되지 않은 경우 경고합니다. 이러한 경고를 인증하려면 항상 최신 버전의 브라우저를 실행하고 있는지 확인하십시오.

>피싱이란: What About Phishing?

보안 사이트는 사이버 범죄자가 귀하의 정보를 가로채지 못하도록 보호할 수 있지만 사이버 범죄자가 피싱 사기를 통해 귀하에게 직접 연락할 수 있다는 점을 알고 있어야 합니다. 많은 피싱 사기는 은행, 신용 카드 회사 또는 기타 금융 기관의 공식 통지처럼 보이도록 만들

어집니다.

사이버 범죄자는 신용 카드 번호 및 기타 계정 정보를 포기하도록 속이기 위해 공식적 것처럼 보이는 이메일을 보내고 신뢰할 수 있는 조직인 것처럼 보이는 공식적인 웹 사이트를 만들 수 있습니다.

개인 정보를 요구하는 금융 기관의 이메일, 팝업, 문자 메시지 또는 전화에 응답하지 마십시오. 문제가 있는지 항상 전화를 해서 확인하십시오.

>안전한 온라인 쇼핑: Safe Online Shopping

온라인 쇼핑은 편리한 쇼핑 방법이며 현장에서 구할 수 없는 제품에 대한 액세스를 제공합니다. 그러나 모든 온라인 금융 거래와 마찬가지로 사기의 가능성이 있습니다. 쇼핑 사이트를 사용할 때는 사이트가 안전한지 확인하고 사용 약관을 주의 깊게 읽고 보안 프로그램을 활용하는 등 일반적인 안전 예방 조치를 실행해야 합니다:

1. Research the Company of Seller
2. Closely Examine the Product
3. Understand the Terms and Costs
4. Pay with a Credit Card
5. Save and Print a Record of the Transaction
6. Enjoy Your Purchased

>온라인 금융거래의 추가적 팁: Additional Tips for Conducting Online Financial Transactions

■ 흔적을 남기지 마라: Leave No Trace

인터넷 사용 기록, 암호 및 기타 개인 데이터가 저장되거나 이후 컴퓨터를 사용하는 사람이 액세스할 수 없도록 항상 개인 브라우징 세션에서 금융 거래를 하는 것을 고려하십시오. 완료되면 웹 사이트에서 로그 오프하고 모든 브라우저 창을 닫으십시오. 그리고 가능하면 공용 또는 공유 컴퓨터 또는 공용 무선 인터넷 연결을 통해 금융 거래를 수행하지 마십시오.



■ 백 버튼 사용시 주의하라: Be Careful with the Back Button

온라인 상점에서 구매하는 경우 사이트에서 구매에 대한 정보를 수집하고 처리해야 합니다. 정보를 입력한 후 뒤로 버튼을 누르면 정보가 다시 전송될 수 있습니다. 사이트에 따라 이로 인해 신용 카드에 두 번 청구될 수 있습니다. 자금을 이체하는 동안 뒤로 버튼을 누르면 은행 사이트에서도 비슷한 일이 발생할 수 있습니다.

실수로 뒤로 버튼을 누르면 브라우저에서 "양식을 다시 보낼" 것인지 묻는 메시지가 자주 표시되며 취소를 클릭하여 다시 보내지 않도록 할 수 있습니다.



[6] Smart Social Networking and Communication Tips

Facebook, Twitter 및 LinkedIn과 같은 사이트를 통한 소셜 네트워킹은 그 어느 때보 다 번성하고 있으며 이제 우리 중 많은 사람들이 온라인 커뮤니케이션에 익숙해졌습니다. 그러나 이 새로운 상호 작용 방식에 너무 민감하기 전에 온라인과 오프라인 모두에서 자신을 보호하기 위해 안전 및 개인 정보 보호와 관련된 문제를 면밀히 살펴볼 필요가 있습니다.

이 강의에서는 온라인에서 안전하고 효과적으로 의사소통하기 위한 전략과 팁을 제공하는 것 외에도 개인 정보 보호와 관련된 현재 문제를 소개합니다. 이 팁에는 프로필을 설정하는 방법, 공유하기 전에 고려해야 할 사항, 사람들을 직접 만날 때 해야 할 일 및 좋은 네티켓을 연습하는 방법이 포함됩니다.

>소셜 네트워킹과 프라이버시: Social Networking and Privacy

웹에서의 소셜 네트워킹과 공유는 우리가 상상하지 못했던 방식으로 도약하고 있습니다. 그러나 모든 재미있는 사회적 측면과 함께 개인 정보 보호에 대한 큰 의문이 존재합니다.

모든 사람들이 소셜 네트워킹이 개인 정보에 미칠 수 있는 결과를 인식해야 하는 이유를 알아보려면 대화형을 고려하십시오.

>소셜 네트워킹 사이트에서 프로필 설치: Setting Up Profiles on Social Networking Sites

대부분의 소셜 네트워킹 사이트에서는 가입할 프로필을 설정해야 합니다. 일부 프로필은 간단하며 웹 사이트의 토론 게시판에 참여할 때와 같이 화면 이름과 이미지만 포함 할 수 있습니다. YouTube 또는 Facebook 페이지와 같은 다른 프로필을 사용하면 창의적이고 정교해질 수 있는 많은 자유를 얻을 수 있습니다. 대화식을 검토하여 프로필에서 자신을 안전하게 표현하는 방법을 알아보십시오.

아무도 귀하의 계정에 액세스할 수 없도록 강력한 암호를 만드는 것을 잊지 마십시오.

>프라이버시 세팅을 검토하라: Review Your Privacy Settings

소셜 네트워킹 사이트에는 개인 정보 보호 설정이 있지만 많은 사람들이 사용자 설정을 지정하지 않거나 설정 방법을 이해하지 못합니다. Facebook은 사용자의 개인 정보를 노출할 수 있는 복잡한 설정이 있는 사이트의 완벽한 예입니다. 이 모든 혼란 속에서 프로파일 보호되는지 어떻게 확인할 수 있습니까?

■ 사이트의 프라이버시 정책을 주의깊게 검토하라: Carefully Review a Site's Privacy Policy

귀하의 정보가 어떻게 표시되고 사용되는지 이해하기 위해 귀하가 가입하는 모든 사이트의 개인 정보 보호 정책을 철저히 검토하는 것이 가장 좋습니다. 개인 정보 보호 정책이 압도적이고 혼란스러운 경우 조사를 수행하고 어떤 종류의 조언이나 자습서가 제공되는지 확인하십시오.

■ 충고나 가르침을 살펴봐라: Look for Advice or Tutorials

관심있는 사이트에 대한 프로파일을 설정하는 방법에 대한 검색을 수행합니다. 특정 사이트에서 개인 정보를 유지하는 방법에 대해 실제로 알아야 할 사항을 알아내는 블로그 또는 방법 자습서가 있는 경우가 많습니다.

■ 스스로를 구글하라: Google Yourself

프로필이 어떻게 표시되는지 확인하는 가장 좋은 방법은 Google 검색에 이름을 입력하는 것입니다.

>네티켓 팁: Netiquette Tips

온라인에서 소통하는 동안 어색하거나 부정적인 경험을 피하기 위해 네티켓의 기본을 아는 것이 도움이 됩니다. 네티켓은 온라인 커뮤니케이션을 위한 네트워크 에티켓을 의미하며 초보자에게 매우 유용할 수 있습니다. 다음은 온라인으로 의사소통 할 때 모든 사람이 연습해야 하는 몇 가지 기본 팁입니다.

■ 존중하여라: Be Respectful

항상 당신이 대우받고 싶은대로 다른 사람들을 대하십시오. 좋은 경험 법칙은 상대방의 얼굴에 기꺼이 말하고 싶지 않은 내용을 온라인으로 전달하지 않는 것입니다.

■ 너무 신속하게 공격하지 마라: Don't Be Too Quick to Take Offense

온라인 커뮤니케이션에서 우리는 일반적으로 얼굴표정을 보거나 신체언어를 판단하거나 목소리 톤을 들을 수 없습니다. 따라서 메시지 나 게시물의 의미를 잘못 해석하기가 매우 쉽습니다. 또한 기술 자체는 우리를 덜 매력적으로 만드는 경향이 있습니다. 공격을 받기 전에 발신자에게 메시지를 명확히 하십시오.

■ **의미전달을 위하여 이모티콘과 약자를 사용하라: Use Emoticons and Abbreviations to Convey Meaning**

어쨌든, 유머 및 의미를 전달하려면 “lol”(큰 소리로 웃음) 또는 “jk”(농담)와 같은 일반적인 약어를 배우거나 :) 또는 :(또는 = 0과 같은 이모티콘을 사용하십시오. 그러나 주의하십시오. 이러한 기호를 남용하면 메시지가 성가시거나 읽기 어려워질 수 있습니다.

■ **타인의 프라이버시를 보호하라: Protect the Privacy of Others**

다른 사람의 사진이나 동영상은 온라인에 게시하기 전에 허락을 받아야 합니다. 또한 전달하는 이메일에서 다른 사람의 이메일 주소를 삭제하여 보호해야 합니다.

■ **철자, 문법, 언어를 체크하라: Check Your Spelling, Grammar and Language**

잘못된 철자, 잘못된 문법 또는 모욕적인 언어를 사용하면 읽기가 불편하고 사람들이 당신을 부정적으로 묘사할 수 있습니다. 메시지를 보내기 전에 잠시 시간을 내어 통신 내용을 확인하고 불쾌하거나 부적절한 언어를 사용하지 마십시오.

netiquette에 대한보다 광범위한 리소스를 보려면 Albion.com 또는 NetworkEtiquette.net을 방문하십시오. 또한 규칙은 이메일, 온라인 채팅, 웹 포럼, 온라인 게임 및 기타 소셜 네트워킹 아울렛에 따라 다를 수 있습니다. 사용중인 특정 콘텐츠와 관련된 특정 규칙을 검색하는 것이 현명 할 수 있습니다.

>**공유하기 전에 생각하라: Think Before You Share!**

온라인으로 소통하고 공유하는 것이 더 편해지면서 우리가 게시하는 내용이 우리를 문제에 빠뜨릴 가능성이 있음을 기억하십시오. 기술의 비 인격적 성격에 대한 어떤 것들은 우리가 개인적으로 대면하지 않을 것 같은 글을 쓰거나 게시하는 것에 대해 안전하다고 느끼게 합니다. 어떤 상황에서는 센드를 누르기 전에 확실히 생각할 필요가 있습니다.



>**대면 모임 때의 예방조치: Precautions to Take When Meeting People Face to Face**

온라인에서 사람들을 알게됨에 따라 실제 세계에서 직접 만나고 싶을 때가 있을 수 있습니다. 온라인에서 누군가와 직접 만나기 전에 예방 조치를 취하는 것이 매우 중요합니다. 범죄자와 사기꾼은 피해자를 직접 만나도록 유인하기 위해 온라인에서 자신의 신원을 쉽게 위조하고 다른 사람으로 가장 할 수 있습니다.

1. **Protect Your Identity**

2. Tell Someone
3. Research the Person
4. Meet in Public
5. Bring a Friend
6. Repeat Until Safe

직접 만나기 전에 전화로 대화할 수도 있지만, 발신자 ID를 차단하거나 Skype와 같은 익명 전화 서비스를 사용하려면 주의해야 합니다. 이 정보는 귀하를 식별하고 찾는 데 사용될 수 있으므로 집 전화를 사용하거나 전화번호를 제공하지 마십시오.

>경고 사인: Warning Signs

직접 만나는 사람들과 문제가 발생하지 않도록 다음 팁을 검토하십시오.

■ 본능을 믿어라:

당신의 직감을 믿고 뭔가 옳지 않다고 느낄 때 주의를 기울이십시오. “위험 신호”와 의심스러운 특성에 주의하십시오. 그 사람이 너무 통제하고 있습니까? 그들은 다른 사람들에 대해 나쁘게 이야기합니까? 특정 질문을 피합니까? 그들은 빨리 화를 냅니까? 당신의 직감은 당신이 누군가와 함께 진행해야 하는지 아니면 즉시 끝내야 하는지에 대한 좋은 척도입니다.

■ 여유를 갖고 처리하라: Take your time and maintain control.

불편함을 느끼는 경우 언제든지 설명할 필요없이 자리를 떠나 통신을 종료할 권리가 있습니다. 당신이 그렇게하는 것에 익숙해지기 전에 다른 사람이 당신을 설득하거나 집적되게 (badger:오소리)하지 마십시오. 사람이 진짜라면, 천천히 일을 해야 할 필요성을 이해할 것입니다.

■ 돈이나 성 얘기를 꺼내면 즉시 빠져 나와라: End things with someone who brings up “sex talk” too soon or asks about money.

이 사람들은 거의 항상 성실하지 않으며 결국 사기를 당하거나 해를 끼칠 수 있습니다.

■ 음주를 피하라:

회의 전이나 회의 중에 술을 마시지 마십시오. 다른 사람을 판단하는 능력과 상황의 안전을 저해 할 수 있습니다.

[7] Cyber-Harassment, Stalking and Addiction

불행히도 우리의 인터넷 사용은 추악해질 가능성이 있습니다. 우리가 생활에 점점 더 기술

을 통합함에 따라 사이버 괴롭힘, 스토킹 및 인터넷 중독의 가능성을 인식해야 합니다.

이 강의에서는 부정적인 커뮤니케이션을 방지하는 방법과 사이버 괴롭힘 및 사이버 스토킹에 대응하는 방법에 대해 설명합니다. 또한 인터넷 중독의 측면을 탐구하고 평가 및 치료를 위한 리소스를 제공할 것입니다

>온라인 대화의 부정적 측면: The Negative Side to Communicating Online

소셜 네트워킹은 전 세계적으로 소통 할 수 있는 좋은 방법이자 관계를 유지하고 사회화하는 재미있는 방법이 될 수 있습니다. 그러나 이러한 형태의 의사 소통에는 단점이 있을 수 있습니다. 익명의 성격과 인터넷의 개방적인 액세스는 공격적이고 경멸적이며 부적절한 커뮤니케이션에 노출될 가능성을 허용합니다. 일반적으로 이러한 유형의 콘텐츠를 무시하거나 노출되는 페이지를 그대로 둘 수 있습니다.

그러나 상황이 갑자기 다음과 같이 확대되는 경우가 있습니다.

>> **Flame Wars** : 의도적으로 모욕적인 진술과 인신 공격이 대화의 초점이 됨

>> **Cyber-Harassment** : 온라인에서 발생하는 모든 종류의 괴롭힘

>> **Cyber-Stalking** : 사이버 스토킹이 자주 사용하는 사이버 괴롭힘. 피해자를 괴롭히는 여러 온라인 리소스 (예: 이메일, 인스턴트 메시지 및 다양한 게시판에 게시된 게시물)

>사이버 괴롭힘과 사이버 스토킹 예방 팁: Tips to Help Prevent Cyber-Harassment and Cyber-Stalking

안타깝게도 이러한 경험은 정신적, 정서적 고통을 야기할 수 있으며 오프라인 또는 “실제”에서 괴롭힘이 될 가능성이 있습니다. 대부분의 사이트에는 이러한 부정적인 콘텐츠에 대한 정책이 있지만, 이에 대응하고 제어할 수 있는 방법이 제한되는 경우가 많습니다. 따라서 이러한 상황이 처음에 발생하지 않도록 다음과 같은 예방 조치를 취하는 것이 중요합니다.

■ 뜨거운 논쟁에 참여하지 마라: Avoid Getting Involved in Flame Wars

의견을 공유하기 전에 생각하는 것이 중요합니다. 특히 논란의 여지가 있거나 종교적이거나 정치적이거나 본질적으로 동의하지 않는 경우에는 더욱 그렇습니다. 이러한 유형의 게시물은 부정적인 반응을 유발할 수 있으므로 신중하게 고려해야 합니다.

■ 이름 노출을 피하라: Avoid Using a Revealing Screen Name

성별 및 연령에 영향을 받지 않고 귀하의 이름이나 귀하에 대한 개인 정보가 노출되지 않는 대화명을 선택하십시오. 선정적이거나 시선을 사로잡는 별명이 있다면 원치 않는 관심의 대상이 될 수 있습니다.

■ 개인정보의 공유를 피하라: Avoid Sharing Personal Information

온라인으로 개인 정보를 공유할 때는 극도로 주의하십시오. 누군가가 귀하에 대해 더 많이 알수록 온라인 및 오프라인에서 귀하에게 더 쉽게 액세스할 수 있습니다.

■ 사이버 괴롭힘과 사이버 스토킹에 대항하라: Responding to Cyber-Harassment and Cyber-Stalking

사이버 괴롭힘 또는 사이버 스토킹 상황에 처한 경우 대응하기 위해 취해야 할 특정 단계가 있습니다. 이 단계의 세부 사항을 배우려면 대화식을 검토하십시오.

>인터넷 중독: Internet Addiction

점점 더 많은 사람들이 온라인에서 더 많은 시간을 보내면서 인터넷 중독이 점점 더 우려되고 있습니다. 인터넷 중독은 일반적으로 인터넷을 강박적으로 사용하는 것으로 정의되며 다음과 같이 건강에 해로운 사용을 포함할 수 있습니다.

- > 온라인 도박
- > eBay와 같은 경매 사이트를 포함한 온라인 쇼핑
- > 온라인 업무를 포함한 온라인 데이트
- > 사이버 포르노 및 사이버 섹스 사이트
- > Facebook 및 Twitter와 같은 소셜 네트워킹 사이트
- > 온라인 게임
- > 오락과 정보를 위한 강박적인 웹 서핑

우리 중 일부에게는 기술을 일상 업무, 가정 생활 및 커뮤니케이션과 통합하기 때문에 인터넷에서 많은 시간을 보내는 것이 필수적인 것처럼 보일 수 있습니다. 그러나 인터넷 사용이 정상에서 비정상으로 언제 바뀌었는지 어떻게 알 수 있습니까?

인터넷 사용이 오프라인 생활을 방해하기 시작하면 문제가 있을 수 있습니다. 징후에는 인터넷에서 시간을 보내기 위해 일, 관계 및 일상적인 책임을 소홀히 하는 것이 포함됩니다. 또한 인터넷에 대한 극도의 감정적 반응이 있는 경우 (예 : 오프라인 상태일 때 불안함을 느끼고 온라인 상태로 돌아왔을 때 행복감을 느끼는 경우) 도움을 구해야 할 수 있습니다.

[8] Wireless and Mobile Device Safety

우리가 인터넷을 사용하기 위해 책상에 묶여 있어야했던 시절은 오래 전입니다. 무선 신호의 광범위한 가용성과 함께 iPad 및 스마트 폰과 같은 장치를 사용하여 이제 언제 어디서나 인터넷에 액세스할 수 있습니다. 그렇다면 이동 중에 어떤 예방 조치를 취해야 할까요?

이 레슨에서는 특히 Wi-Fi 핫스팟에서 인터넷 위협으로부터 무선 네트워크 및 모바일 장치를 보호하기 위한 팁을 배웁니다. 모바일 장치 예의를 연습하는 방법을 배웁니다. 또한 운전 중 모바일 기기 사용 전략을 논의합니다.

>무선 네트워크 보안: Wireless Network Security

무선 네트워크 (Wi-Fi라고도 함)를 사용하여 인터넷에 액세스하는 경우 안전한지 확인해야

합니다. 그렇지 않으면 해커와 사이버 범죄자가 모든 활동과 정보에 액세스할 수 있습니다. 무선 네트워크 보안은 매우 기술적일 수 있으므로 초보자는 인터넷 서비스 제공업체 (ISP)의 도움을 받는 것이 좋습니다. 무선 보안을 설정할 때 다음 팁을 고려하십시오.

>와이파이 집중지역의 보안 팁: Wi-Fi Hotspot Safety Tips

Being able to access the internet through Wi-Fi hotspots in coffee shops, hotels, airports, etc. can be quite convenient. However, these Wi-Fi hotspots are often not as secure as your home network. Review the following interactive to learn how to stay safe when connecting to a public network.

- 집의 경계를 넘어서 감지되지 않도록 신호 강도를 제한하십시오.
- SSID 브로드 캐스팅을 비활성화하여 네트워크가 신호 범위 내에서 다른 무선 사용자에게 보이지 않도록 합니다.
- 강력한 암호를 사용하십시오. 기억하기 쉽지만 다른 사람이 추측하기 어려운 암호 또는 암호를 선택해야 합니다.
- MAC (Media Access Control) 주소 필터링을 활성화하여 무단 무선 클라이언트가 네트워크에 침입하는 것을 방지합니다.
- 네트워크에서 WPA (Wi-Fi Protected Access) 또는 WPA2를 사용하는지 확인하십시오.
- WPA 대신 이전 WEP (Wired Equivalent Privacy)를 사용하는 경우 암호화를 최대화해야 합니다.

>모바일 기기의 보안: Mobile Device Safety

최근 몇 년 동안 휴대폰은 훨씬 더 강력해져 인터넷 검색, 이메일 확인, 프로그램 다운로드 등을 할 수 있습니다. 그러나 이러한 새로운 기능은 또한 바이러스 및 기타 맬웨어의 위험이 더 커지고 개인 정보에 대한 위험이 있음을 의미합니다. 모바일 장치를 사용할 때는 컴퓨터에서 사용하는 것과 동일한 주의를 기울여야 합니다.

>악성웨어 피하는 방법: Tips for Avoiding Malware

Norton 및 Kaspersky와 같은 일부 회사는 휴대폰에서 실행할 수 있는 바이러스 백신 소프트웨어를 제공하지만 잠재적으로 휴대폰 기능을 저하시킬 수 있으므로 조사를 수행합니다. 다음은 모바일 장치에서 맬웨어를 방지하는 데 도움이 되는 몇 가지 팁입니다.

- 휴대폰을 최신 상태로 유지하십시오. 휴대 전화 확인 보안 업데이트 다운로드에 대한 지침은 제조업체 웹 사이트를 참조하십시오.
- 프로그램이나 앱을 다운로드 할 때 주의하십시오. 프로그램이나 앱에 맬웨어가 포함되어 있을 수 있으므로 다운로드하기 전에 조사하세요.
- “무료 제공” 및 “무료 벨소리”를 피하십시오. 벨소리 또는 보안 업데이트와 같이 다운로드할 소프트웨어를 제공하는 이메일 또는 인스턴트 메시지는 맬웨어가 포함될 수 있습니다.

- 뭔가 의심스러워 보이면 본능을 믿으십시오.

>프라이버시의 유지: Privacy on the Go

개인 정보 보호가 중요하다면 기기에 설치하는 앱에 세심한 주의를 기울여야 합니다. 항상 서비스 약관 및 개인 정보 보호 정책을 검토하여 그들이 귀하의 정보를 어떻게 사용하는지 여부를 알 수 있습니다. 앱에서 해당 옵션을 제공하는 경우 개인 정보 설정을 사용자 지정할 수도 있습니다.

또한 이미 배운 개인 정보 보호 문제 (예 : 지리적 위치)와 이러한 문제가 모바일 장치에서의 경험에 어떤 영향을 미칠 수 있는지 다시 생각해 봐야 합니다. 이는 소셜 네트워킹 앱 및 활동을 추적하는 기타 앱에 특히 중요합니다.

>무선 및 모바일 기기의 예의: Wireless and Mobile Device Courtesy

새로운 무선 기능과 iPad 및 스마트 폰과 같은 고급 모바일 장치를 통해 우리는 언제 어디서나 통신하고 미디어에 액세스할 수 있습니다. 그러나 이러한 새로운 기술은 점점 더 방해가 되고 있으며 때로는 문제가 되는 행동에 기여할 수 있습니다. 방해가 되는 벨소리, 시끄러운 대화 및 무례한 문자 메시지는 다른 사람을 방해하고 성가시게 하며 화를 낼 수 있습니다.

>산만한 운전: Distracted Driving

모바일 기기에서 대화, 서핑, 문자 메시지 중 운전과 관련된 사고의 수가 크게 증가하고 있습니다. 그렇다면 우리 대부분은 위험에 대한 압도적인 증거에도 불구하고 이러한 활동에 계속 참여하는 이유는 무엇입니까? 다음을 고려하세요:

- 복수의 일을 할 수 있다고 믿는다: We believe we can multi-task.

뇌는 활동 중 하나가 운전하고 음악을 듣는 것과 같이 수동적이거나 비대화형인 경우 한 번에 하나 이상의 활동에 참여할 수 있습니다. 그러나 우리의 두뇌는 운전하고 전화를 거는 것과 같이 동시에 사고하고 반응해야 하는 두 가지 상호 작용에 참여할 수 없습니다.

한 활동은 항상 다른 활동에 대해 무시되어 우리를 위험에 노출시킵니다.

- 타인보다 운전을 잘 한다고 믿는다: We believe we are better drivers than others.

우리는 다른 사람들의 휴대 전화로 말하면서 무모하게 운전하는 것에 대해 화를 낼 수도 있지만, 우리는 우리가 더 나은 운전자라고 믿고 그것을 해낼 수 있다고 믿습니다. 실제로 우리도 운전이 잘되지 않는지만 “부주의 실명(inattention blindness)”은 우리가 알아 차리지 못하게 합니다.

- 대응력이 뛰어나다고 믿는다: We believe we have to respond.

오늘날의 즉각적인 액세스 세계에서 우리는 지속적으로 사용할 수 있어야 한다고 믿습니다. 따라서 전화 나 문자 메시지를 무시하는 것은 들어 본 적이 없는 것처럼 보일 수 있습니다. 또한 우리 중 일부는 우리가 원한다고 말하는 땡땡(ring)이나 빙(bing) 소리를 들을 때 약간

의 “흥분(rush of excitement)”을 느낍니다. 불행히도 이러한 정서적 욕망은 우리가 안전하도록 경고하는 우리 뇌의 합리적인 측면을 압도하는 것 같습니다. I

자신과 다른 사람의 안전을 위해 대화형을 검토하여 모바일 장치를 사용하고 운전하는 동안 안전을 유지하는 방법을 알아보십시오. 산만한 보행으로 인한 사고도 증가하고 있습니다. 위에 나열된 것과 동일한 많은 이유때문에 걷거나 모바일 장치를 사용하는 것도 건강에 해로울 수 있습니다.

>휴대전화와 암: Cell Phone Radiation and Cancer

연구 증가로 인해 휴대폰과 암, 특히 뇌암과의 연관성에 대한 관심과 논쟁이 증가하고 있습니다. 휴대폰과 다른 무선 장치는 암의 원인으로 간주되는 저주파 “비열(non-thermal)”방사선을 방출합니다. 현재 세계 보건기구, 미국 암 학회, 국립 암 연구소, 식품의약국은 모두 휴대폰의 사용이 공중 보건 위험을 초래하지 않는다고 하였습니다. 그러나 그것들의 특히 장기간 노출과 관련된 주제에 대한 지속적인 연구를 지원하고 있습니다.

-FIN-