OUCH! | 2015 년 11 월호

컴퓨터 사용자를 위한 월간 정보보호 인식 뉴스레터

OUCH!

이달 호 주제..

- 가짜 온라인 쇼핑몰
- 사용 컴퓨터/모바일 기기
- 신용카드

# 안전한 온라인 쇼핑 방법

## 연말 주의보

연말이 다가옴에 따라, 전세계 수 백만명의 사람들이 멋진 선물을 찾고 있다. 많은 사람들이 멋진 것을 찾아서 긴 줄 및 붐비는 것을 피하기 위해 오프라인 매장보다 온라인 쇼핑을 이용한다. 하지만 이러한 시기에는 사기범들이 온라인 또는 금융사기를 하기에도 가장 좋은 때이다. 이번 호는 온라인 쇼핑의 위험과 예방법에 대해서 알아본다

**객원 편집자**

Jonathan Homer (@JonathanLHomer) 정부 및 민간부문 모두에서 사이버보안 인식제고의 유명한 리더이다. 조나단은 청중 관련사항 및 첨단 교육 기법 전문가이다.

## 가짜 온라인 쇼핑몰

대부분의 온라인 몰은 합법적이지만, 일부는 범죄자들이 만든 가짜 웹사이트이다. 사기꾼들은 다른 사이트나 유명 사이트의 상품을 복사해서 가짜 웹사이트를 만듭니다. 사기꾼들은 이러한 가짜 웹사이트를 이용해서 최저가 상품을 찾는 사람들을 먹이감으로 삼습니다. 만약에 온라인에 "완전 최저가"를 검색해보면, 이러한 가짜 웹사이트로 이동될 수 있습니다.

원하는 상품을 구매하기 위해 어떤 웹 사이트를 선택해야 할 때, 다른 곳보다 상품 가격이 굉장히 저렴하거나 이미 다른 곳에서는 품절된 상품을 판매하는 사이트는 조심해야 합니다. 그 상품이 굉장히 저렴한 이유는 물건을 구매한 후에 가짜 상품 또는 훔친 물건을 받거나 또는 일부는 아예 배달도 되지 않기 때문입니다. 다음사항을 통해 우리자신을 보호해 보십시요.

- 상품 판매 또는 지원관련 질의를 받을 수 있는 정확한 우편 주소, 전화번호가 있는 지 확인해야 합니다. 사이트가 의심스러우며, 전화로 확인바랍니다.
- 문법이나 철자에 오류가 있는 등의 이상한 점이 있는 찾아보시기 바랍니다.
- 웹 사이트가 과거에 방문한 적이 있는 유명한 웹사이트를 정확하게 모사했는데, 웹사이트의 도메인명이나 쇼핑몰의 이름은 조금씩 다른 것이 보이면 유의하시기 바랍니다. 예를 들어 아마존 쇼핑을 위해http://amazon.com 웹사이트를 방문하곤 하였는데, URL http://store-amazon.com로 아마존과 유사한 웹사이트가 있는 것을 발견하면 의심을 해야 합니다.
- 검색엔진에 쇼핑몰 이름 또는 URL을 쳐서, 다른 사람들이 과거에 그 웹사이트에 대한 평가를 확인해 볼 필요가 있습니다. "사기", "절대로 이용 안함" 또는 "가짜"와 같은 단어를 찾아 보시기 바랍니다. 후기가 없다는 것은 좋은

## 안전한 온라인 쇼핑 방법

징조가 아니며, 웹사이트가 새로운 것이라는 것을 의미합니다.

사이트가 전문적으로 보인다고 해서 진짜가 아니라는 점을 기억해야 합니다. 사이트가 어떤 면에서 이상하다고 느끼면 좀더 세밀하게 봐야 합니다. 이상하다고 느끼면, 사용하지 마시기 바랍니다. 대신 믿을 수 있는 유명한 웹사이트를 이용하거나, 과거에 이용한 사이트를 이용하시기 바랍니다. 유명한 사이트는 좋은 가격이 없거나, 좋은 행사가 없을 수 있지만, 합법적인 제품을 받을 수 있습니다.

안전한 온라인 쇼핑방법은 평판이 좋은 믿을 만할 온라인 쇼핑몰을 이용하는 것입니다.

### 사용 컴퓨터/모바일 기기

합법적인 웹사이트에서 쇼핑하는 것뿐만 아니라, 온라인 쇼핑몰을 이용할 때는 사용하는 컴퓨터 또는 모바일 기기가 안전한지도 확인해야 합니다. 사이버 범죄자들이 컴퓨터나 모바일 기기를 감염시켜, 은행 계좌, 신용카드 정보 및 패스워드를 수집하고 있습니다. 기기를 안전하게 만들기 위해 다음 단계를 따르기 바랍니다.

집에 어린이가 있다면 컴퓨터를 두 대를 이용해서, 한대는 어린이 전용, 한대는 부모용으로 하는 것이 좋습니다. 어린이들은 호기심이 많고, 기술을 이용하는 것을 좋아해서 악성코드 같은 것에 쉽게 감염됩니다. 컴퓨터나 태블릿을 분리하여 한대는 온라인 뱅킹 및 쇼핑과 같은 온라인 거래용으로만 사용하면, 감염될 위험을 낮출 수 있습니다. 컴퓨터 두 대를 사용하지 못하면 컴퓨터 한대에 계정을 따로 만들어서 아이들이 관리자 계정을 사용하지 못하도록 해야 합니다.

- 당신의 아이 하나는 성인을위한 하나 : 당신이 당신의 집에 자녀가있는 경우, 두 장치를 고려해보십시오. 아이들은 호기심과 기술을 상호 작용이다.그 결과, 자신의 장치를 감염시킬 가능성이 높다. 바로 그러한 온라인 뱅킹 및 쇼핑 등의 온라인 거래를위한 별도의 컴퓨터 나 태블릿을 사용하면 감염 될 가능성을 줄일 수 있습니다. 별도의 장치가 옵션이 아닌 경우, 공유 컴퓨터에 별도의 계정을 가지고 자녀가 관리 권한이없는 보장합니다.
- 금융 거래 시 가정용 네트워크 또는 신뢰할 수 있는 무선 AP 등 직접 관리하는 무선 네트워크에만 접속해야 합니다. 커피숍과 같은 공공 와이파이에서는 뉴스를 보는 것은 괜찮지만, 은행 계좌에 접속하는 것은 위험합니다.
- 항상 최신의 운영체제로 업데이트하고, 최신의 안타바이러스(AV) 소프트웨어를 운영하시기 바랍니다. 이렇게만 해도 범죄자들이 기기들을 감염시키기가 어려워 집니다.

### 신용카드

매달 오는 신용카드 명세서를 꼼꼼히 읽어보고 이상한 사용내역이 있는 지 확인해야 합니다. 적어도 한 달에 한 번은 명세서를 검토해야 합니다. 일부 신용카드 회사들은 한도가 초과되는 경우나, 신용카드 사용내역을 이메일이나

## 안전한 온라인 쇼핑 방법

스마트폰으로 알려주는 기능을 제공합니다. 다른 방법은 온라인 구매용 신용카드를 정해서, 카드정보가 해킹되면 다른 결제에 영향을 주지 않고 바로 그 카드를 바꿀 수 있습니다. 사기가 발생하였다면, 신용카드사에 즉시 전화해서 상황을 설명하고 결제 취소요청을 합니다. 그래서 온라인으로 결제 시에는 신용카드가 직불카드보다 훨씬 안전합니다. 직불카드는 은행 계좌에서 바로 돈이 빠져 나갑니다. 그래서 사기 결제라는 것을 알았더라도 돈을 다시 돌려받는 것이 굉장히 어렵습니다.

마지막으로 신용카드 번호를 노출하지 않고 결제할 수 있는 새로운 기술이 있습니다. 신용카드사는 온라인 구매할 때마다 별도의 유일한 카드 번호를 만들어 주는 서비스가 있습니다. 또는 미국 같은 경우에는 페이팔(PayPal) 같은 서비스는 온라인 결제 시 신용카드 번호를 입력하도록 요구하지 않습니다.

### 자세히 알아 보기

http://www.securingthehuman.org를 방문해서 OUCH! 뉴스레터를 읽어 보시고, 월간 OUCH! 정보보호지식 뉴스레터를 구독하십시오. 그리고 SANS 정보보호지식 솔루션에 대해서 좀 더 알아보시기 바랍니다.

### 한글판

본 문서는 한국의 ITL(http://www.itlkorea.kr)에서 번역하였습니다. ITL 은 미국 SANS 연구소의 한국 파트너로서 IT 거버넌스 및 IT 보안 분야의 최신의 지식과, 양질의 교육과 세미나를 진행하는 교육기관입니다. 추가적인 사항은 itl@itlkorea.kr 로 문의해주시기 바랍니다.

### 참고자료

| | |
|---|---|
| 패스워드: | http://www.securingthehuman.org/ouch/2015#april2015 |
| 2단계 인증: | https://www.securingthehuman.org/ouch/2015#september2015 |
| 탑 5 패스워드 관리프로그램: | http://lifehacker.com/5529133/five-best-password-managers |
| SANS 일일 보안팁: | https://www.sans.org/tip_of_the_day.php |



편집위원회 : Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner, 번역: 진수희(ITL Inc.)