신종 온라인 사기 피싱 대처법

사용자 교육 등 적극적 예방 노력 최선

최근 들어 온라인상에서는 신종 사기가 위력을 더해가고 있다. 조금만 허점을 보이면 사용자의 지갑을 털어가 버리는 '피싱'이 바로 그것. 호환마마보다 더 무서운 피싱에 걸려들지 않기 위해선 각별한 주의가 요망되지만, 무작정 조심한다고 해서 피싱의 공격을 피해갈 수 있을까. 대답은 물론 '아니오'다. 피싱에 대한 피해를 최소화하기 위해서는 갈수록 지능화돼 가는 공격 유형을 잘 파악하고 미리 대비하는 것이 최선책이다. 이에 최근 늘어나는 피싱 공격 유형 및 기술에 대해서 검토해보고 이에 따른 대응 방법을 살펴본다.

글 **한이** 자유기고가

"저희 은행의 인터넷뱅킹 보안 시스템을 강화했습니다. 고객님께서는 저희 은행 홈페이지에 접속하신 후 개인정보를 확인해 주시기 바랍니다." 어디서 많이 본 듯한 문구일 것이다. 바로 신종 인터넷 금융사기를 위한 피싱 이메일의 한 예다.

얼마 전부터 국내에서도 은행 홈페이지와 비슷한 가짜 웹 사이트를 개설한 뒤 비밀번호와 아이디를 빼내 실제 계좌에서 돈을 인출해 달아나는 이른바 '피싱' 사기가 속출하고 있어 최근 금융당국이 소비자 경보를 발령키도 했다.

금융감독원은 "인터넷 사이트를 통해 은행 직원을 사칭, 불법으로 돈을 빼 내가는 금융사기가 지난 9월부터 한달여 만에 5건이 발생해 1억6,986만원의 예금이 불법 인출됐다"며 "현재까지 밝혀진 피해사례 외에 더 많은 피해자가 있을 것으로 예상됨에 따라 소비자들의 각별한 주의가 필요하다"고 당부한 바 있다.

금감원에 따르면 사기단의 범행수법은 네이버와 다음 등의 인터넷 사이트에 개인 신용에 관계없이 즉시대출을 해준다는 광고를 게재 한 후 이를 보고 찾아온 사람을 피싱 대상으로 삼았다고 한다.

이처럼 '피싱'은 최근 들어 그 공격이 점점 더 지능화되고 교묘해지고 있을 뿐만 아니라 매우 광범위하게 퍼지고 있어 IT 전문가가 아닌 일반 소비자들도 알 수 있는 일반적인 용어가 돼가고 있다.

한국정보보호진흥원(KISA)에 따르면 지난해 자체 접수한 국내 위장 홈페이지 신고 건수만도 총 220건으로, 월 평균 18건의 보안 취약 사이트가 해외 피싱사고의 경유지로 악용된 것으로 나타났다. 올해 1월에는 61건이 신고돼 지난해에 비해 급증하는 추세를 보였으며, 6월에는 100건을 넘어섰다고 한다. 이러한 신고 건수의 증가는 보안이 취약한 일부 국내 웹 서버들이 해킹을 당해 외국 금융기관, 쇼핑몰 등의 위장 홈페이지로 악용되는 사례가 증가했음을 의미한다. 또한 앞서 언급했듯이 실제 피해사례까지 속출하고 있어 이에 대한 대응책 마련 요구가 한층 높아지고 있다.

실제로, 안티피싱 워킹그룹(APWG)에 따르면 우리나라는 올해 4월 기준 경유지로 악용된 서버를 보유한 국가 순위에서 3위를 차지했다고 한다. 그렇다면 국내에서 이렇게 피싱이 광범위하게 확산되는 이유는 무엇일까. 또 나날이 지능화되는 피싱의 공격에 어떻게 대응해야 할까. 이를 검토하기 위해서는 피싱이 웜 바이러스 등의 다른 위협 요소들과 어떤 차이점이 있고, 어떻게 배포되는지를 먼저 살펴봐야 할 것이다.

국내도 피싱의 안전지대 아니다

피싱이 웜 바이러스 등과 같은 여타의 위험 요소들과의 큰 차이를 보이는 것은 바로 공격 이후의 의도다. 대부분의 바이러스, 웜 및 기타 악성 프로그램 제작자들은 사용자의 컴퓨터나 파일에 손상을 입히거나 이를 무차별적으로 확산시킴으로써 명성을 얻고 싶어 하는데 반해 피싱 공격을 가하는 피셔들은 사용자의 하드웨어와 소프트웨어 손상에는 그다지 관심이 없으며, 해커로서의 명성에도 관심이 없다. 피싱은 이러한 하드웨어 및 소프트웨어의 손상이나 명성보다는 보안 감시망 하에서

의 금융 사기를 통해 금전적인 이득을 취하는데 그 목적이 있다.

명성을 추구하는 다른 악성 프로그램 제작자들과 경쟁하는 대신 이들은 인터넷의 힘을 이용해 보다 효과적인 방법을 통해 금전적인 가치가 있는 정보를 빼내는데 집중한다. 때문에 피싱 시에는 실제로 두 개의 온라인 신분이 함께 도용된다. 전형적인 피싱 공격은 인증 프로그램처럼 보이는 이메일과 가짜 웹 사이트 이 두 가지로 구성된다. 특히 피싱 이메일의 경우 일반적으로 수신자들을 당황스럽게 하거나, 혼란 또는 우려를 야기할 수 있도록 계좌 오류, 계좌 확인, 보안 업데이트 · 업그레이드 및 일상적인 신제품 · 서비스 제공 등의 제목으로 뿌려지고 있다. 그 이후 메일을 받은 수신자들은 이메일 본문에 제공된 링크를 클릭하는 등 즉각적으로 반응하게 되고 이 링크는 수신자들을 피싱 웹 페이지로 이동토록 유도하는 방식이다.

피싱 웹 사이트를 통한 공격도 비슷한 맥락이다. 가짜 웹 사이트에 동일한 회사 로고 · 그래픽 · 필체 · 폰트 · 레이아웃 등을 통해 대부분 진짜처럼 보이게 위조하고 이렇게 위 · 변조된 웹 페이지에는 사용자가 자신의 금융 인증 번호를 입력하는 GUI를 포함시켜 도용된 모든 정보를 익명의 원격 사용자에게 바로 전송하는 방식이다.

이처럼 피싱이 이메일이나 웹 사이트를 통한 공격 양상을 보여 전문가들은 피싱을 통상 스팸의 변종으로 간주한다. 이는 피싱이 주로 SMTP 및 표준 인터넷 프로토콜의 치명적인 결함으로 인해 가능한 이메일 스푸핑 기술을 사용하고 있기 때문이다. 하지만 최근의 피싱 공격은 스팸에 비해 보다 발전된 방식의 분산 속임수와 기술을 사용, 고유한 신분 도용 루틴을 추가함으로써 스팸 위험보다 한 단계 업그레이드된 위험도를 보이고 있다.

이는 피싱 기술이 갈수록 발전하고 있다는 얘기다. 초기의 피싱 신용 사기는 간단한 ASCII 텍스트로 작성돼 일반적인 이메일과 거의 다를 바가 없었다. 즉, 당시에는 사용자에게 개인 정보를 유출하도록 요구하는 정도여서 상대적으로 피해가 적었다. 하지만 시간이 지남에 따라 매우 전문적인 느낌의 복잡한 신용 사기로 발전하고 있는 것. 일례로, 이전의 단조로웠던 ASCII 이메일들은 전문화된 HTML 기반의 메일로 대폭 교체됐고, 여기에 더해 폰트 유형 · 색상 · 화려한 그래픽까지 완벽하게 위장하기 위한 여러 요소들을 포함하기에 이르렀다. 대부분 실제로 정보를 수집하는 웹 사이트 링크를 포함한다. 이러한 사이트 역시 똑같이 복제한 위장 사이트로 만들어 사용자들이 자신의 개인 정보를 유출하도록 유혹하고 있다.

백 엔드 부문에서의 정보 수집 또한 더욱 복잡해졌다. 이전에는 스크립트 키들이 개인적 사용을 위해 신용 카드 번호를 획득하는 정도였는데 반해 현재 피싱 신용 사기는 도용 정보를 수집, 대조 및 이용하는 데 있어 조직적이고 체계적인 방법을 사용하고 있다. 대표적인 예가 저작권과 등록된 상표와 똑같이 위조된 로고와 상호 등을 활용해 합법적으로 보이게 하는 피싱 이메일들이다. 심지어 최근의 피싱 이메일 중 일부는 피싱 공격에 대한 경고문까지 포함하고 있어 공격 대상자를 현혹시키고 있을 뿐만 아니라 실제 은행 고객에게만 이메일을 보내는 표적 기술을 결합해 피싱 공격의 성공을 증가시키고 있다.

피싱 기술 및 공격 유형

그러면 이제부터 보다 구체적으로 오늘날 많이 활용되고 있는 피싱 기술에 대해 살펴보자. 현재 많이 활용되고 나타나고 있는 피싱기술은 대략 5가지 유형으로 구분된다.

● 명백한 피싱 URL 표시

가장 쉽게 그 위조 여부를 식별할 수 있는 기술로 이 경우에는 피셔들이 실제 피싱 URL을 숨기려고 노력하지 않기 때문에 피싱 URL이 주소 표시줄에 명백하게 표시된다. 일부의 경우, 합법적 도메인과 유사한 도메인 이름을 사용하기도 한다.

● 주소 표시줄 스푸핑

합법적 주소를 표시하기 위해 브라우저의 주소 표시줄을 바꾸는 기술이다. 효과는 피싱 URL 위에 하얀색 배경의 텍스트로 합법적 은행 주소를 나타내지만 웹 페이지의 등록정보를 확인하면 가짜 사이트의 실제 주소가 나타난다.

● 팝업 창 사용

이 기술은 백그라운드에서 합법적 웹 사이트를 여는 스크립트를 사용하는 것이다. 가짜 팝업 창은 대부분 합법적 웹 사이트와 동일하며 포그라운드에서 바로 열린다. 사용자로 하여금 팝업 창이 공식 페이지와 직접 연관됐다는 생각이 들도록 유도하는 경우다. 팝업 창이 합법적 웹 사이트의 일부만 차지하는 경우도 있다.

● 피싱 이메일의 형식 사용

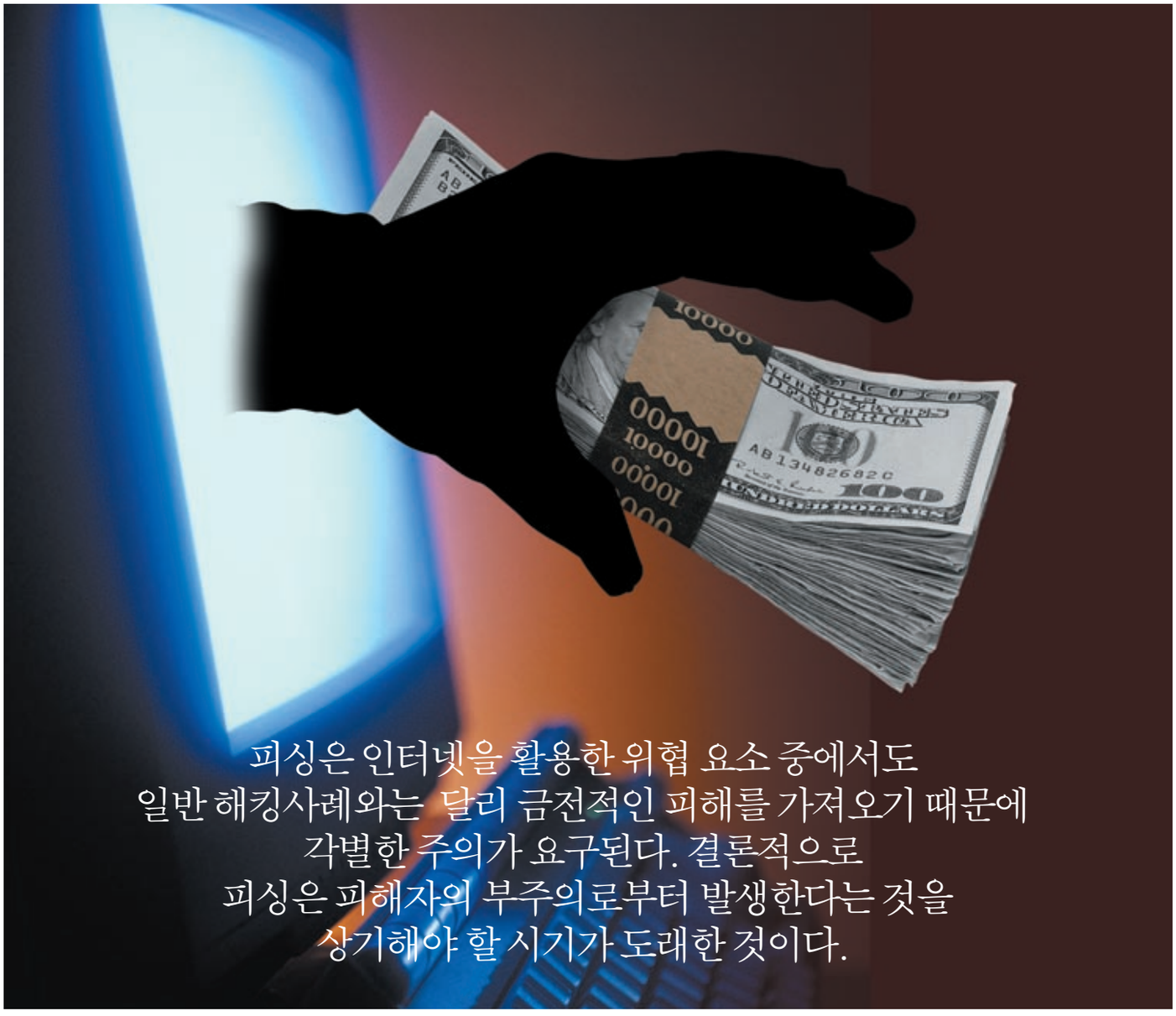
HTML 형식으로 전송되며 사용자로부터 개인 계정 정보를 수집하는데 사용되는 임베디드 형식이 이미 포함돼 있는 기술이다. 도용된 세부 정보는 지정된 이메일 주소로 전송되거나 특정 웹 사이트에 게시된다.

● 웹 사이트 스푸핑

합법적이고 믿을 수 있는 사이트를 그대로 복제하는 것이 가장 어렵고 발전된 공격기법 중 하나다. 위조 웹 사이트는 실제 사이트의 세부적인 사항까지 완전히 일치한다. 위조 사이트에 나타나는 모든 링크들은 하나의 피싱 도메인으로 연결된다.

이와같은 피싱 신용사기 공격의 영향에는 어떤 것이 있을까. 우선 피싱은 앞서도 언급한 바와 같이 일반적인 웜 바이러스의 위협과는 달리 금전적인 목적이 있기에 도난 당한 은행 계정 정보가 가장 중요한 공격 대상으로 이용될 수 있다.

피셔는 피해자의 계정에 합법적으로 액세스한 후 계정 암호를 변경, 계정에 대한 합법



피싱은 인터넷을 활용한 위협 요소 중에서도
일반 해킹사례와는 달리 금전적인 피해를 가져오기 때문에
각별한 주의가 요구된다. 결론적으로
피싱은 피해자의 부주의로부터 발생한다는 것을
상기해야 할 시기가 도래한 것이다.

적 사용자를 효과적으로 차단한 후 사용 가능한 자금을 임시 계정으로 이체하고 피해자가 이 사실을 알기 전에 인출한다. 특히 이들은 종종 피해자를 대신해 가짜 수표를 발행하기도 한다. 또한 수집된 신용 카드 증명서를 사용해 인증되지 않은 온라인 구독이나 구매를 하는 경우도 있다. 피해자는 엄청난 금액의 청구서를 보거나 신용 카드 사용 시 한도초과 메시지를 듣게 됐을 경우에나 이러한 사실을 알게 될 수밖에 없는 구조다.

이외에도 피셔들은 카드 번호, PIN 및 만료일과 같은 ATM 계정 정보를 사용해 복제 ATM 카드를 만들 수도 있고 이를 활용해 개인 계정의 잔액을 인출해 갈 수도 있으며, 유출한 개인 정보를 온라인 언더그라운드 커뮤니티를 통해 판매하기도 한다. 즉, 피싱 공격의 영향은 계정이 비어버린 개별 피해자에서 끝나지 않고 지속적인 개인 정보의 무단 도용의 남발을 낳는다. 때문에 피싱은 모든 피싱 공격에 이용되는 은행 등 기업의 신용도를 떨어뜨린다. 비즈니스에서 상호명은 모든 기업에게 가장 중요한 자산이고 고객에게 믿음을 제공하는 첫걸음이다. 피싱 공격으로 인해 이에 대한 신뢰가 쉽게 무너질 수 있다는 얘기다.

사용자 교육의 필요성

결국 피싱 공격이 성공하면 비즈니스 수행의 한 가지 방법인 인터넷에 대한 사람들의 신뢰를 점점 잃게 만든다. 모든 면에서 피싱은 풍요롭고 편리한 삶을 향상시키는 인터넷 기술에 대한 잠재적인 성장과 발전을 저해하는 요소가 되고 있는 것.

특히 피싱 신용 사기는 일반적으로 패치가 제공되지 않은 시스템에서 URL 변경이 가능한 특정 마이크로소프트 윈도 시스템에서 가장 많이 나타나기 때문에 이를 차단하기 위한 방어기술 도입의 필요성이 높아지고 있다.

하지만 피싱 차단 기술을 도입했다고 완벽하게 안전한 것도 아니며 무작정 조심한다고 해서 해결될 문제 역시 아니다. 피싱의 공격 유형을 잘 파악하고 미리 대비하는 것이 가장 중요하다. 특히 전문가들은 피싱의 경우 사용자 교육이 반드시 뒷받침돼야 한다고 강조한다. 피싱 성공의 범위가 실제로 이메일을 받는 사용자에게 달려있기 때문이다. 이에따라 피싱과 관련해서는 사용자 교육이 가장 우수한 방어법이며, 이와 관련한 보안지침들이 다양하게 제시되고 개발되고 있는 실정이다.

그렇다면 피싱 공격으로부터의 대응력을 높이며, 피싱 위협으로부터 벗어날 수 있는 팁은 어떤 것들이 있는지 점검해보자. 이는 공격 대상자에 따라 개인 차원의 대응 방법과 기업 차원의 대비책으로 나눠 살펴볼 수 있다.

피싱 예방 체크 리스트

● **개인사용자 대응법**

- 피싱 이메일은 사용자들의 즉각적인 응답을 유도하기 위해 수신자를 당황 또는 흥분하게 만들도록 설계됐음을 상기하고 계정 인증 정보를 요청하는 이메일 메시지를 받으면 신중하게 대처한다.
- 신용 카드 번호와 같은 중요한 정보를 제출하는 경우, 방문한 웹 사이트가 보안성이 유지되는 사이트인지 해당 사이트의 보안을 확인한다.
- 스푸핑이 의심되는 전자 메일의 내부 링크를 클릭하지 않고 그 대신 브라우저의 주소 표시줄에 합법적인 회사 URL을 직접 입력해 합법적인 회사의 사이트로 직접 이동하고 그 곳에서 로그인한다. 혹은 해당 사이트 회사에 직접 전화로 문의해 본다.
- 의심스러운 피싱 이메일 메시지의 첨부 파일은 개인 정보를 훔칠 수 있는 악성 프로그램을 실행시킬 수 있으므로 열지 않도록 하고, 되도록 의심스러운 웹 사이트의 온라인 거래는 하지 않는다.
- 인터넷뱅킹을 이용할 때는 항상 지정된 계정을 사용토록 하고 인터넷에서 피싱에 관한 최신 뉴스 및 정보를 조사한다.
- 사용자 브라우저를 업데이트하고 항상 보안 패치를 신속하게 적용, 최신 버전으로 유지한다.
- 피싱 공격은 분산 및 실행의 목적으로 여러 악성 프로그램 및 스파이웨어 프로그램에 링크될 수 있다. 따라서 피싱 공격뿐만 아니라 악성 프로그램 및 해커 침입을 보호할 수 있는 최신 버전의 바이러스 백신 등 개인용 보안 소프트웨어를 설치하고, 설치된 보안 소프트웨어를 항상 업데이트한다.
- 개인 방화벽을 설치해 해커 침입을 탐지한다.
- 피싱 관련 웹 브라우저 툴바를 설치한다. 피싱 사이트가 팝업 형태로 돼 있다면 피해를 막을 수 있다.
- 피싱으로 인한 피해를 입었을 경우 혹은 의심이 가는 피싱 공격을 받았을 경우, 한국정보보호진흥원 홈페이지(www.kisa.or.kr)에 접속하거나 사이버범죄 신고센터, 피싱 워킹 그룹 등에 접속해 해당 피싱 공격에 대해 신고한다.

● **기업사용자 대응법**

기업의 경우에도 개인사용자를 위한 피싱 대응책들이 마찬가지로 적용되며 위에 언급한 사항 이외에 다음과 같은 지침이 추가된다.

- 기업 이메일 정책을 제정 · 시행한다.
- 눈에 띄는 안티 피싱 정보 캠페인을 정기적으로 시행한다.
- 피싱에 관한 소비자 교육을 지원한다.
- 직원들의 메일함에 피싱 이메일이 수신되지 않도록 믿을 수 있는 보안 소프트웨어 제공업체로부터 안티 피싱 제품 및 서비스 구매를 고려한다.

보안수준 향상이 자산 보호의 길

지금까지 피싱기술, 공격 유형, 그리고 피싱 위협으로부터 벗어날 수 있는 예방법 및 방어대책까지 살펴봤다. 이상과 같이 과거에는 기술적인 모방 또는 모조를 통해 사용자의 신분을 도용하거나 위 · 변조했지만 수 세기가 지난 오늘날에는 방치된 정보를 찾기 위해 다른 사람의 편지함, 서랍 및 심지어 휴지통까지 뒤지는 세상이 됐다. 인터넷의 발전이 우리에게 편리함을 가져다 준 것은 사실이지만 그에 따른 폐해도 다양하다.

특히 피싱은 인터넷을 활용한 위협 요소 중에서도 일반 해킹사례와는 달리 금전적인 피해를 가져오기 때문에 각별한 주의가 요구된다. 결론적으로 피싱은 피해자의 부주의로부터 발생한다는 것을 상기해야 할 시기가 도래한 것이다. 즉, 사용자가 얼마만큼의 주의를 기울이느냐에 따라 피싱의 공격에 대응하는 폭은 상당히 달라질 수 있다는 얘기다.

보낸 사람이 불분명하거나 의심 가는 메일을 받을 경우, 특히 거래 은행을 사칭해 개인의 금융관련 정보를 입력하도록 요구하거나 '대박 투자정보 제공' 등 금전상의 이익을 미끼로 사이트 방문을 유혹하는 메일인 경우에는 반드시 사실을 확인하는 등 사용자 스스로가 세심한 주의를 기울이는 게 우선돼야 한다. 현재 국내에는 3,000만명이 넘는 인구가 인터넷뱅킹을 사용하고 있을 정도로 IT 인프라가 잘 갖춰져 있고 인터넷이 발달되어 있지만 보안에 있어서는 갈수록 사각지대가 되는 경향이 있다. 인터넷이라는 기술이 제공하는 편리함과 효율성은 애석하게도 이를 통해 금전적인 이익을 추구하고자 하는 일부 옳지 못한 사람들에게도 또다른 길을 제공하게 됐고 그것이 피싱이라는 공격으로 현실화됐다.

때문에 편리함을 추구하는 동시에 조금만 주의를 기울여 정보보호 마인드를 강화해야 할 것이다. 그래야만 피싱 사고로 인한 금전적 피해의 예방은 물론이고 안전하게 따뜻한 진정한 의미의 디지털 세상을 향유할 수 있을 뿐만 아니라 자신의 소중한 정보 자산을 지켜낼 수 있게 될 것이다. 새로운 기술을 적용하는 것 만큼이나 사용자 스스로 보안수준을 높이는 인식 제고가 절실하다.