피싱 사기를 알아채고 피하는 방법

사기범은 이메일이나 문자 메시지를 통해 당신을 속여 개인정보를 빼냅니다. 하지만 이런 피해를 예방할 수 있는 여러가지 방법이 있습니다.

피싱 사기를 알아채는 방법

사기범은 이메일이나 문자 메시지를 통해 당신을 속여 개인정보를 빼냅니다. 이들은 당신의 비밀번호, 계좌번호, 혹은 사회보장번호를 노릴 것입니다. 이런 정보를 빼내는데 성공하면 이들이 당신의 이메일, 은행, 혹은 기타 계좌에 접근할 수 있게 됩니다. 사기범은 매일같이 수천 건의 피싱 공격을 감행합니다. 그리고 꽤 자주 성공합니다. FBI 인터넷범죄신고센터(Internet Crime Complaint Center)에 따르면 피싱 사기 피해액이 일 년에 5,700만 달러에 이른다고 합니다. 사기범은 사기 수법을 자주 업데이트 합니다. 그래도 피싱 이메일이나 피싱 문자 메시지를 알아챌 수 있는 몇 가지 신호들이 있습니다.

피싱 이메일과 피싱 문자 메시지는 당신이 알고 있거나 신뢰하는 기업에서 보낸 것처럼 위장합니다. 은행, 신용카드 회사, 소셜 네트워킹 사이트, 온라인 지불 웹사이트나 애플리케이션, 혹은 온라인 쇼핑몰에서 보낸 것처럼 보입니다. **피싱 이메일과 피싱 문자 메시지는 보통 특정 링크를 클릭하거나 첨부파일을 열어보도록 유도합니다.** 거기에 이런 내용이 적혀 있을 수 있습니다.

- 의심스러운 활동이나 로그인 시도를 감지했다고 합니다
- 당신의 계좌 혹은 지불 정보에 문제가 있다고 합니다
- 일부 개인정보를 확인해 달라고 요청합니다
- 허위 청구서를 보냅니다
- 특정 링크를 클릭해 돈을 지불하도록 유도합니다
- 정부로부터 환급 받을 돈이 있으니 등록을 해달라고 요청합니다

- 공짜 사은품 쿠폰을 제공합니다

실제 피싱 이메일 사례를 하나 보여 드리겠습니다.

받은 편지함에 이런 이메일이 와 있다고 가정해 보십시오. **피싱 이메일이라는 낌새가 보이시나요?** 한 번 살펴봅시다.

- 이 이메일은 넷플릭스에서 보낸 것처럼 보입니다. 당신이 알고 있고 신뢰하는 회사입니다. 넷플릭스 로고와 헤더도 사용했습니다.
- 이메일에는 결제에 문제가 있어 계정이 보류 중이라는 설명이 있습니다.
- 이 이메일은 "Hi Dear"라는 일반적인 인사말로 시작합니다. 넷플릭스 계정이 있는 사람이라면 알겠지만 이 회사는 이메일을 보낼 때 이런 인사말을 쓰지 않습니다.
- 이 이메일은 지불 상세정보를 업데이트하라며 링크를 클릭하도록 유도하고 있습니다.

언뜻 보면 이 이메일은 진짜 같아 보이지만 절대 진짜가 아닙니다. 이런 이메일을 보내는 사기범은 해당 회사와 무관합니다. 피싱 이메일을 통해 사기범에게 개인정보를 넘겨주는 사람들은 실질적인 피해를 입을 수 있습니다. 그리고 명의를 도용 당한 기업의 평판도 훼손될 수 있습니다.

피싱 공격을 피하는 방법

이메일 스팸 필터를 이용해 받은 편지함에서 많은 피싱 이메일을 걸러낼 수 있습니다. 하지만 사기범은 항상 스팸 필터를 뚫기 위해 애쓰기 때문에 추가적인 보호책을 마련하는 것이 좋습니다. 피싱 공격에 피해를 입지 않기 위해 여러분이 취할 수 있는 4단계 조치를 소개합니다.

피싱 공격을 막는 4단계 조치

1. 보안 소프트웨어를 이용해 당신의 컴퓨터를 보호하세요. 소프트웨어 자동 업데이트를 활성화하여 소프트웨어가 새로운 보안 위협에 대응할 수 있게 해 주세요.

2. 휴대폰의 소프트웨어 자동 업데이트를 활성화하여 휴대폰을 보호하세요. 소프트웨어 업데이트는 보안 위협으로부터 휴대폰을 보호하는 중요한 역할을 합니다.

3. 다단계 인증을 통해 당신의 계정을 보호하세요. 어떤 계정들은 로그인을 할 때 두 가지 이상의 인증 절차를 요구합니다. 이를 다단계 인증(multi-factor authentication)이라고 합니다. 계정 로그인 시 필요한 추가적인 인증 절차는 다음 두 가지 범주로 나뉩니다.

- 문자 메시지 혹은 인증 애플리케이션을 통해 받는 암호 등
- 지문, 망막, 얼굴 등을 이용한 생체 스캔

다단계 인증을 이용하면 사기범이 당신의 사용자명과 비밀번호를 갖고 있는 경우에도 쉽게 로그인을 할 수 없습니다.

4. 데이터를 백업해서 보호하세요. 데이터를 백업하세요. 백업된 데이터가 홈네트워크와 연결되어 있으면 안됩니다. 컴퓨터에 있는 파일을 외장 하드 드라이브나 클라우드 저장공간에 복사해둘 수 있습니다. 휴대폰에 있는 데이터도 백업하세요.

피싱 공격이 의심되는 활동을 포착했을 때 대응 방법

특정 링크를 클릭하거나 첨부파일을 열도록 유도하는 이메일 혹은 문자 메시지를 받았다면 이런 질문을 한 번 던져 보세요. **내가 이 회사의 계정을 갖고 있나? 아니면 발신인이 내가 아는 사람인가?**

그 답이 "아니오"라면 피싱 사기일 가능성이 있습니다. 위에서 설명한 피싱 사기를 알아채는 방법을 다시 읽어보고, 피싱 사기의 단서를 찾아보세요. 찾았다면 해당 이메일 혹은 문자 메시지를 신고한 다음 삭제하세요.

그 답이 "예"라면 해당 회사의 실제 전화번호나 웹사이트를 통해 연락해 보세요. 이메일에 적힌 정보는 이용하지 마세요. 첨부파일과 링크를 클릭하면 유해한 멀웨어가 설치될지도 모릅니다.

피싱 이메일에 응답을 했을 경우 대처 방법

사기범이 당신의 사회보장번호, 신용카드번호, 혹은 은행계좌번호를 빼냈다는 의심이 들면 IdentityTheft.gov를 클릭하세요. 도난당한 정보의 유형에 따라 취할 수 있는 구체적인 조치들이 설명되어 있습니다.

이미 링크를 클릭했거나 첨부파일을 열어서 유해한 멀웨어가 설치되었다고 의심되면 컴퓨터 보안 소프트웨어를 업데이트하세요. 그 다음에 보안 소프트웨어로 컴퓨터를 검사해 보세요.

피싱 신고 방법

피싱 이메일이나 피싱 문자 메시지를 받으면 신고해 주세요. 제공해주신 정보는 피싱 사기를 막는데 큰 도움이 됩니다.

1단계. 피싱 이메일을 받았다면 피싱방지실무그룹(Anti-Phishing Working Group)의 이메일 주소 reportphishing@apwg.org로 전달해 주세요. 피싱 문자 메시지를 받았다면 전화번호 SPAM(7726)으로 해당 메시지를 전달해 주세요.
2단계. ftc.gov/complaint를 통해 피싱 공격을 FTC에 신고하세요.

태그: 사이버 보안, 피싱, 사기 2019년 5월