SECURE OUR WORLD

온라인 범죄자들보다 더 똑똑하게

간단한 세 가지 팁으로 피싱 사기를 방지하세요

피싱 사기는 신뢰할 수 있는 출처에서 보낸 것처럼 보이도록 설계된 온라인 메시지입니다. 안전한 이메일, 첨부 파일 또는 이미지라고 생각한 것을 열어보았다가 멀웨어나 개인 데이터를 노리는 사기꾼에게 노출될 수 있습니다.
다행히 중요한 데이터를 보호하기 위한 예방 조치를 취할 수 있습니다. 피싱을 감지하고 신고하여 디바이스와 데이터를 보호하는 방법을 알아보세요.

1 일반적인 징후 **파악하기**

- 긴급하거나 감정적으로 호소하는 언어
- 개인정보 또는 금융 데이터 전송 요청
- 예기치 않은 첨부 파일
- 신뢰할 수 없는 단축 URL
- 발신자로 추정되는 이메일 주소와 일치하지 않는 이메일 주소
- 문법/철자 오류(흔하지 않음)

2 거부 및 신고

피싱 스팸

"스팸 신고" 기능을 사용하여 의심스러운 메시지를 신고하세요. 메시지가 신뢰할 수 있는 기관과 유사하게 디자인된 경우, 해당 기관의 웹페이지에 있는 연락처 정보를 사용하여 해당 기관에 신고하세요.

3 삭제하기

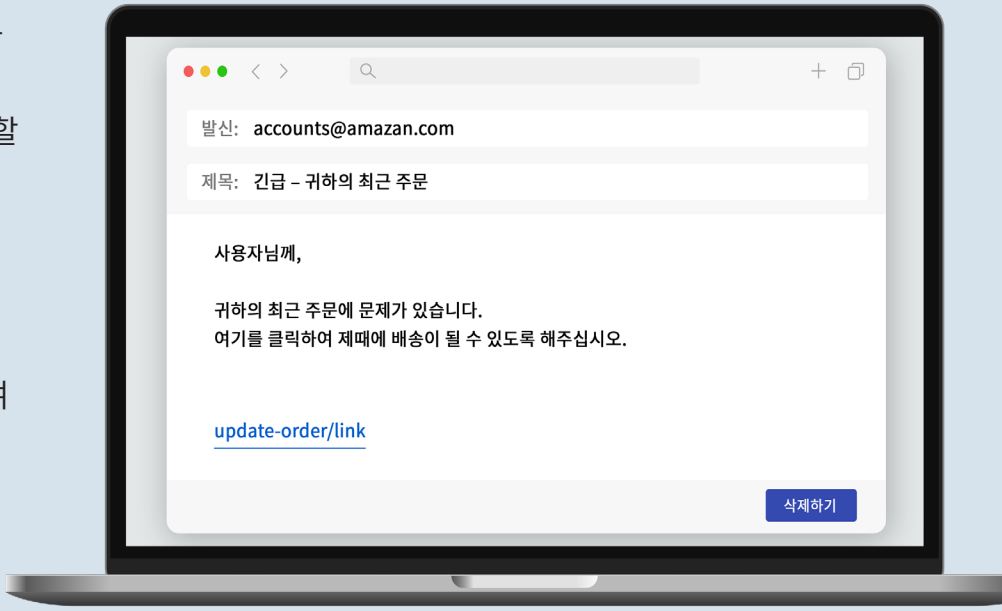
해당 메시지를 삭제합니다. "구독 취소" 링크를 포함한 첨부파일이나 링크를 클릭하거나 답장하지 마세요. 수신거부 버튼에는 피싱에 사용되는 링크가 포함될 수도 있습니다. 삭제하기만 하면 됩니다.

삭제하기

의심스러운 메시지라면 피싱 메시지일 가능성이 높습니다.

하지만 실제일 가능성이 있더라도 링크나 첨부파일을 클릭하거나 번호로 전화를 걸지 마세요. 회사나 개인에게 직접 연락할 수 있는 다른 방법을 찾아보세요:

- 회사 웹사이트로 이동하여 연락처 정보를 찾아보세요.
- 등록된 번호로 해당 사람에게 전화하여 메시지를 보냈는지 확인합니다.



피싱을 피하는 것이 안전한 **세상을 만드는 한 가지 방법입니다.**

우리 모두

온라인에서 더 안전하게 지낼 수 있도록 서로 도울 수 있으니, 이 팁을 가족이나 친구와 공유하세요!

cisa.gov/SecureOurWorld