

의심스러운 이메일을 처리하는 방법

자신의 조직을 사이버 범죄자로부터 지키려면 의심스러운 이메일을 처리하는 방법을 아는 것이 중요합니다. 의심스러운 이메일을 올바르게 처리하지 못하면 피싱 공격의 피해를 입을 수 있습니다.

아래의 팁에 따라 의심스러운 이메일을 올바르게 처리하세요.

이메일에 회신하지 말 것

지인에게서 온 듯한 의심스러운 이메일을 받았을 경우, 자세한 내용을 알아보려고 이메일에 회신하고 싶은 유혹이 들 수 있습니다. 그러나 그 이메일에 회신할 경우 보안 위험이 커질 수 있습니다. 이메일 계정이 해킹되었다면 여러분이 보낸 이메일에 회신하는 사람은 전혀 다른 사람일 가능성이 큼니다. 실제로는 사이버 범죄자가 상대일 수 있습니다.

이메일을 전달하지 말 것

모르는 링크나 첨부파일은 절대 클릭하거나 열지 않는 것이 좋습니다. 그러나 피싱 이메일에 속아서 악성 링크를 클릭했거나 악성 첨부파일을 열면 링크 또는 첨부파일이 예상과 다르게 작동할 것입니다. 예를 들어 의심스러운 이미지 첨부파일을 열 경우 파일에서 설치 창이 열릴 수 있습니다. 또는, 악성 링크를 클릭할 경우 가짜 로그인 페이지로 연결될 수 있습니다.

링크 또는 첨부파일이 의심스러울 경우 동료에게 이메일을 보내 도움을 받고 싶을 수도 있습니다. 그러나 이메일을 동료에게 전달하면 위험이 커집니다. 링크를 클릭하거나 첨부파일을 열었을 경우 비정상적으로 동작하면 위험 신호라고 생각하세요. 정상적이지 않거나 의심스러운 이메일을 절대 다른 사용자에게 전달하지 마세요. 피싱 이메일을 전달할 경우 동료가 피싱 링크를 클릭할 수 있기 때문에 보안 침해의 위험이 커집니다.

이메일을 스팸으로 표시하지 말 것

일반적으로 스팸 이메일이란 원치 않는 광고를 의미합니다. 스팸 이메일이 짜증스러울 수는 있지만 대개는 무해합니다. 그러나 피싱 공격은 정상적인 메시지처럼 보이는 악성 이메일입니다. 일반적으로 피싱 이메일에는 링크 클릭, 첨부파일 열기, 심지어 송금과 같은 행동 유도가 포함됩니다.

의심스러운 이메일을 스팸으로 표시할 경우 이 이메일은 동일한 발송자가 보낸 다른 이메일과 함께 다른 폴더로 이동됩니다. 따라서 의심스러운 이메일을 스팸 폴더로 이동하면 이메일이 숨겨집니다. 그러나 문제는 해결되지 않습니다.

안전을 지키기 위한 팁

의심스러운 이메일을 처리하는 가장 좋은 방법은 자신의 조직에 이메일을 신고하는 것입니다. 이메일을 신고하면 IT 팀에서 위협을 평가하고 완화할 수 있습니다.

의심스러운 이메일을 받으면 아래의 팁에 따라 안전을 지키세요.

- 조직의 의심스러운 이메일 신고 절차를 따릅니다. 사이버 보안 프로토콜을 따르면 모든 사람의 정보를 안전하게 지키는 데 도움이 됩니다.
- 이메일을 신고하는 방법을 모를 경우, 받은 편지함에 이메일을 두고 관리자나 상사에게 도움을 요청합니다.
- 이메일이 스팸인지 피싱 공격인지 구분할 수 없을 경우, 이메일을 신고하면 IT 팀에서 상황을 처리합니다.

