



만화로 보는

알기 쉬운 해킹 메일 대처법



이메일 보안관리는 본인만이 가능하며,
작은 주의로 나의 사생활을 지킬 수 있습니다.

관계부처 합동

[이메일 보안관리에 관한 홍보]

당신을 노리는 해킹메일! 작은 주의로 막을 수 있습니다

해킹 사고의 대부분은
직장 동료나, 정부 조직 등을 사칭해 악성코드를 숨긴 첨부파일이나
가짜 웹사이트 링크 등이 포함된
이메일 공격으로 이뤄진다는 사실을 알고 계십니까?

해킹된 이메일은 개인정보 및 자료유출, 자산절취 등
금전적, 정신적 피해를 야기할 수 있어
보안관리에 각별한 주의가 필요합니다.

이에 정부는 관계부처 합동으로
대표적인 해킹메일 수법으로 피해를 입은 사례와 사고원인을 소개하고
그에 따른 대처법을 알려드리고자 합니다.

무심코 클릭한 해킹메일이
나와 조직의 보안에 치명적인 피해를 줄 수 있음을 이해하고
소소하지만 확실한 이메일 보안 관리에 동참해 주기를 바랍니다.

목차

피해사례 및 사고원인



이메일 공(公)과 사(私) 구분하기

개인일은 개인메일, 업무는 업무메일을 이용하세요

- 피해사례** 공과장의 중요 업무자료 유출 사고 1
- 사고원인** 잘못된 패스워드 입력으로 인한 이메일 자료 유출 3



첨부파일 실행은 꼭 필요한 경우에만

불필요하거나 잘모르는 이메일의 첨부파일은 실행하지 않기

- 피해사례** 김과장의 신용카드 결제 사기 사고 5
- 사고원인** 생각없이 실행한 첨부파일, 내PC는 해커 맘대로 7



믿을 만한 사람이 보낸 이메일도 다시 한번 확인하기

정부가 보냈어도 사전 또는 사후 안내 없이 실행하지 않기

- 피해사례** 박교수의 PC 악성코드 감염 사고 9
- 사고원인** 정부 관계자 사칭 메일에 속아 악성코드 실행 11

해킹메일 대처법



소소하지만 확실한 이메일 보안관리

- 해킹메일 판별법 13
- 이메일 수신 시 유의사항 14
- 이메일 발신 시 유의사항 15

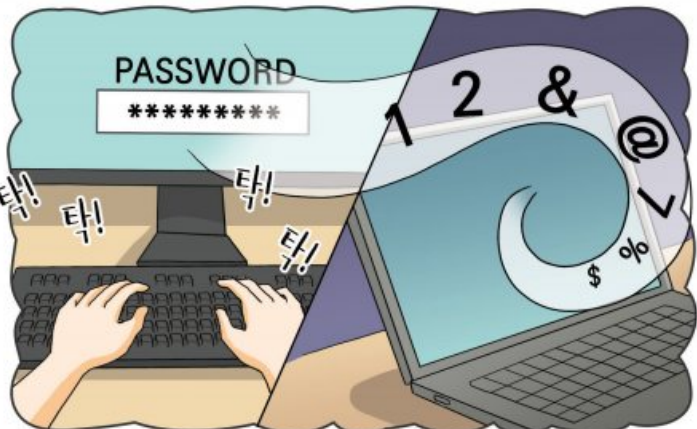


공과장의 중요 업무자료 유출 사고





잘못된 패스워드 입력으로 인한 이메일 자료 유출







김과장의 신용카드 결제 사기 사고



카드 사용내역 상세

거래일시	2019-01-22 03:32
공급가격	5,000,000 원
가맹점명	멋지구리

결제된 데가 해외 쇼핑몰 사이트 같은데?

거래일시	2019-01-22 03:32
------	------------------

거래된 시간도 한국 시간으로 새벽이야. 이 시간에는 자고 있었는데 뭘 소리야!



생각없이 실행한 첨부파일, 내PC는 해커 맘대로







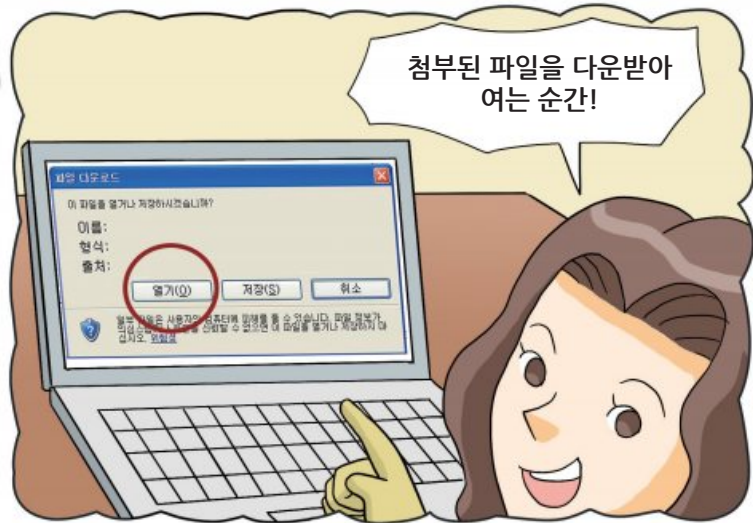
박교수의 PC 악성코드 감염 사고





정부 관계자 사칭 메일에 속아 악성코드 실행





소소하지만 확실한 이메일 보안관리

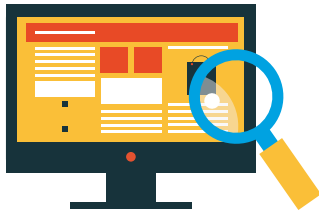


이메일을 이용한
해킹 공격!
알아두면 피할 수
있습니다!

[해킹메일 유형]

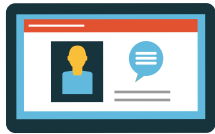
1. 해커는 피해자의 메일주소를 인터넷, 명함 및 SNS를 통해서 입수
2. 국내·외 정세, 업무 관련 메일로 위장해 관공서나 지인 등을 사칭해 유포

:: 해킹메일 판별법 ::



1) 메일주소가 이상하지 않은지 먼저 확인해보세요!

예시 @naver.com -> naver-com.cc
@google.com -> @goog1e.com
@daum.net -> @dauum.net



2) 모르는 사람에게 온 메일 궁금해 하지 마세요!

예시 OO이벤트 당첨, 항공권 파격 특가!



3) 사전에 안내되지 않은 메일 열람하지 마세요!

예시 경찰 출석요구서, 국내·외 정세 자료, 정책 자료, 각종 업무 메일 등



4) 믿을 수 없는 첨부 파일 절대 열람하지 마세요!

예시 이력서, 송장·Invoice, 연말정산 자료, 연봉계약서 등



5) 클릭 할까? 말까? 함부로 클릭 금지!

예시 본문내용 상세보기, 비밀번호 변경하기, 메일함 용량 초과 등의 내용



나의 작은 주의로 이메일 보안은 지킬 수 있습니다.

:: 이메일 수신 시 유의사항 ::

이메일을 안전하게 수신하는 방법은 아래와 같습니다!



1) 백신 설치 및 최신업데이트

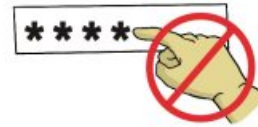
- 바이러스 백신 소프트웨어 설치 및 최신유지
- 운영체제(OS) 및 업데이트 포함

2) 로그인 보안 강화

- 이메일 비밀번호 수시 변경
- 문자(SMS), 모바일OTP(mOTP)등 2단계 인증 로그인설정



PASSWORD



3) 의심메일 열람금지

- 예정되지 않은 업무 메일, 스팸 메일 등 열람금지
- 의심 메일 수신시 발신자에게 유선 및 문자로 확인

4) 패스워드 입력금지

- 이메일에 링크된 홈페이지를 통한 비밀번호 입력금지
- 패스워드 변경은 해당 홈페이지에 직접 방문



5) 첨부파일 실행주의

- 보안 메일 또는 사전 인지시에만 실행
- 그외의 경우에는 발송자에 확인 후 실행

6) 로그인 이력 수시점검

- '로그인 이력' 조회를 통해 비정상 로그인 수시 확인
- '해외 로그인 차단' 기능 적극 활용



의심 메일을 열람했을 경우는 해당 기관 정보보안담당관 또는 국가정보원(111@ncsc.go.kr / ☎111), 한국인터넷진흥원(www.krcert.or.kr / ☎118), 경찰청 (www.cyber.go.kr / ☎182)로 신고해 주세요!

:: 이메일 발신 시 유의사항 ::

이메일 보안 관리는 본인만이 가능합니다.
따라서 **작은 주의**로 **당신의 사생활**을 지킬 수 있습니다.



업무메일 외부 전송 금지

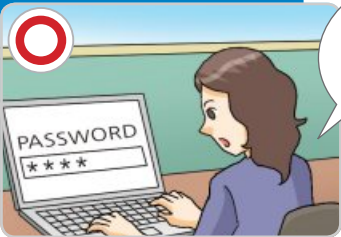


피곤한데 남은 작업은
메일로 보내서 집에서
작업해야겠다~



! · 업무 관련 메일이나 첨부파일을
개인메일로 전송금지!

보안메일 전송



업무 메일은
비밀번호를
설정해야겠어!



! · 업무 메일은 발송 시 보안메일로
전송할 것!
· 유추하기 힘든 비밀번호,
열람 횟수 및 기간 등 설정

메일 발송 안내



방금 메일을
보냈습니다.
확인 부탁드립니다~



! · 업무 관계자에게 유선 및 문자로
사전 또는 사후 안내

만화로보는 알기쉬운해킹메일 대처법

인 쇄: 2019년 6월

발 행: 2019년 6월

발행처: 과학기술정보통신부, 국가정보원, 국방부
교육부, 외교부, 통일부,
문화체육관광부, 경찰청,
한국인터넷진흥원

