정보 윤리 소책자

피싱

【 목표와 포인트】

1) 피싱에 의한 피해와 가해 이해.

   ○ 스푸핑에 의한 피해와 가해의 예제에 대해 생각한다.

2) 피싱의 구체적인 수법을 이해한다.

3) 피싱에 대한 대책에 대하여 생각하고 다음 사항에 주의한다 .

   ○ 메일 발신 주소가 정확하다고는 할 수 없는 것을 이해한다.

   ○ Web에서 ID · 비밀 번호를 보낼 때 그 Web 페이지가 SSL 지원 (https://로 시작하는 URL)임을 확인한다.

   ○ 봇(bot) 같은 바이러스에 감염되지 않도록 바이러스 방지한다.


야~~
야~~
마사미~
오늘
내 피부
짱 촉촉해
보이지
않아?
뭐?
화장수라도
바꾼거야?
정답~!
이거이거
온라인숍
에서
20% 할인!!
마사미도
어때?
거기 사이트는
화장품숍인데
포인트도
모을 수 있고
싸고 강추야!
하...
우~론
?
결제는
어떻게해?
카드로 되나?
응~
얼마전에
학생카드
만들었거든
지불은 항상
후불이지만
말야...
아무래도
좋지만...
그걸
다 먹어??
우와!!!!!
깜짝
!!


모야~
잠깐
이 메일
좀 봐봐!
야~
깜짝
놀랬잖아~
?
축하드립니다.
이 메일은 항상 빅북마트를 이용해
주시는 고객 중에서 추첨을 통해
당첨된 분에게만 보내드리고 있습니다.
항상 이용해 주셔서 감사드립니다.
고객님께서는 캐시백 캠페인에
첨되셨습니다.
아래의 필수입력사항을 작성해
주시면 현금 50만원 상당의 캐시백을
받을 수 있습니다.
현금 50만원을
준다고!?
굉장한걸?
빅북마트라면
나도 CD를
신적이 있어~!
우와~
굉장한데
평소 행동이
좋아서
그런건가?
좋..겠..다..
50만원
들어오면
초코파르페
사줘~~~
OK!
앗싸!
좋은건
빨리!!
http://www.bigbookmart.com/car
http://www.bigbookm
클릭!!


빅북마트
지금 빅북다트에서
현금 50만원 캐쉬백행사중입니다.
여러분의 응모를 기다리고 있으니
많은 참여 부탁드립니다.
음..
빅북마트
전용
페이지네...
하긴...
빅북마트가
확실하긴
하네..
빅북마트
앗싸~!
이거 다 입력하고
전송만하면,
50만원을 준데~
앗싸~~~
그럼..
카드
번호가...
4521이
유효기간
인가...
초코
파르페
~~~~
근데..
잠까만
카즈야..
??




뭐야~
마사미도
초코파르페
사줄께~~~~
안심해!!
그게
아니라...
카즈야..
온라인으로
물건 구입할때
항상
원클릭으로
구입하지
않았어?
응 맞아...
요즘 다른
사이트들도
일일이 매번
입력하는
경우는 없지...
그러면..
왜 일부러
여기서 또
개인정보를
입력시키지?
음..
그러게..
당첨이라
다른거아냐?
난 뽑힌
사람이니까!!
이럴땐..
가르쳐줘
루시~~
이 캠페인
수상하지
않아요??
~~~~


해 설 편
카즈야군 이번엔 마사미덕에 무사했네요~
이런 사칭메일과 같은 피생엔 주의가 필요해요

피.....싱.....????

그럼, 조선생님의 피싱강좌~
출~ 발~!!


Phishing
타인을 사칭한 메이이나 위장한 웹페이지로 인한 온라인 사기를 피싱이라고 합니다.
낚시를 뜻하는 fishing과 위장수법의 정교화를 위미하는 sophisticated가 합쳐져서 fhishing이 되었다는 설도 있어요.


인터넷은 얼굴을 확인 할 수 없으니 피싱과같은 사기를 하기 더 쉬운 환경이라고 할 수도 있어요

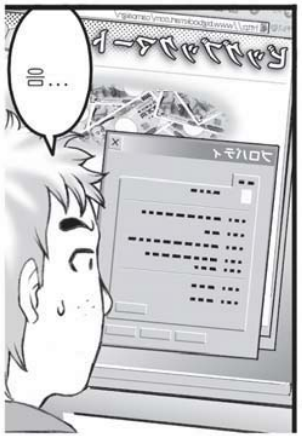

만약에..

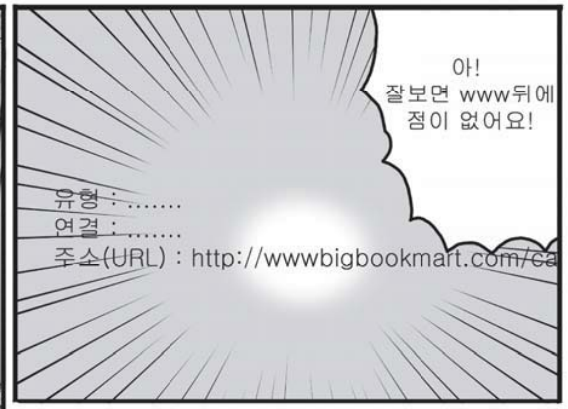

카즈야군이 그대로 신용카드 정보를 입력했다면 사기꾼에게 악용 당할뻔 했어요
그런 일이..


덧붙여서 말하면, 그 캠페인 웹페이지의 URL을 한 볼까요?


http://www.bigbookmart.com/ca
별로 수상한건 없은것 같은데요?


그럼 다음에 화면에서 오른쪽 마우스를 클릭하고 페이지 속성에서 URL을 확인해봐요


음...


아!
잘보면 www뒤에 점이 없어요!
유형 : .....
연결 : .....
주소(URL) : http://wwwbigbookmart.com/ca


그래,
이상하지?
URL을 속여서
표시하거나
디자인을 똑같이
만들어도
원래 기업의
진짜 도메인을
사용하기는
어려워
그래서 진짜
비슷하게 만든
도메인을 쓰고
속이려고 하는
거군요...
그럼,
메일 발신자의
주소는 어떻게
되어 있을까?
음..
그건..
어라? 발신자 주소는
확실히 빅북이라고
되어 있는데요?
발신자 : info@bigbookmart.com
.....
그건 수신한 메일에
적혀 있는 주소죠~
실제로 보낸 사람의
정보는 헤더 정보를
표시해 보면 알게
될꺼에요.
아..
그럼.
Received:from yah-hou-free.com([XXX.
by mailg12.m_free.com with ESM
for <shunshun@m_free.com>;We
Message-ID:.
20417XXXX:mail.yah-hou-free.com
nfo@bigbookmart.com
어라?
야후 도메인에
개인메일
이네요?


알겠지?
수상한
메일이 오면
헤더정보도
꼭 확인해
봐야해요~
피싱수법도
나날이 진화
하고 있어서
개인정보를 입력해야할때
이상하다 싶으면 속성을
살펴보고 꼭 주의해야
해요~!!
네!
그것도 그렇지만...
카드정보와 같이
개인정보를 입력하는
등의 소중한 개인정보를
입력하는 페이지에선
송신중에 그 정보를
제 3자에게 보이지
않도록 하기 위해
정보를 암호화 하는
경우가 대부분입니다
그런 암호화 되어있는
페이지는 그림과 같이
브라우저에 열쇠마크가
표시 되어 있으니까
꼭 확인해 주세요!

용어

【자료】

피싱

회원대상의 사이트나 금융 기관 등의 사이트로 위장하여 이용자에게 사용자ID와 비밀번호, 암호번호, 신용카드 번호 등을 입력시켜 그것을 훔치는 사기이다. 수법으로는 전자 메일로 가짜 메일 주소를 사용하거나 가짜의 웹 사이트를 그럴 듯하게 나타내는 일 등이 있다. 전자 메일의 송신처를 속이는 것은 어렵지는 않으므로, 정보를 입력하기 전에 그 정보가 정말인가 입력의 필요가 있는 것일지 등을 확인을 하는 것이 중요하다.

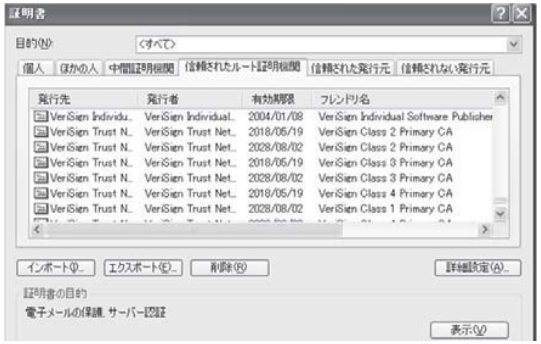
증명서(공개암호증명서)

통신을 암호화하는 웹 사이트(URL이, https://로부터 시작되는 것)에는 화면에 열쇠 마크가 표시되고 있다. 그 열쇠 마크를 클릭 혹은 더블 클릭하는 것으로 증명서를 표시할 수 있다. 증명서로부터는 업데이트의 유무, 증명서의 유효기한, 올바른 URL 등을 볼 수 있다. 각자 한번은 확인해 두면 좋다.

아래의 그림과 같이, 각PC에는「신뢰받은 증명 기관」이라는 기본적인 증명서가 인스톨되어 있다. 이것에 의해 증명서를 신뢰할 수 있는 것인가 아닌가의 판단을 간편하게 실시할 수 있도록 하고 있다.

봇(BOT)

컴퓨터 바이러스의 일종이며 감염시킨 컴퓨터를 네트워크 상에서 조종하는 것을 목적으로 작성된 프로그램. 감염한 컴퓨터가 가짜의 웹 사이트가 되어 알지 못하는 사이에 피싱 사기를 도와주고 있는 경우도 있기에 주의가 필요하다.



피싱의 구체적인 수법 예시

피싱 사기는 우선 정규 기업을 위장한 메일이 보내지는 경우가 많다.
①회원대상의 사이트나 금융기관 등의 사이트로 위장하고 이용자에게 메일을 보낸다. 그 메일에는 계약의 변경, 불량의 갱신, 캠페인이나 서비스의 제공 등의 내용이 쓰여져 있다. 동시에 웹 사이트에의 링크나 첨부 파일 등이 포함되어 있다. 첨부 파일을 사용하는 수법에서는 해당기업의 공식 어플리케이션(application)으로 위장하고 첨부된 실행 파일을실행시키도록 만든다. 예를 들면 은행의 경우에는 인터넷 은행용 어플리케이션(application) 소프트로 가장하거나 뉴스 사이트의 경우에는 기사 리더 어플리케이션(application)으로 가장하거나 한다. 어느 쪽의 경우에도 믿도록 만들기 위해 정규 기업의 로고나 진짜 웹 사이트 혹은 진짜와 아주 닮은 가짜 웹 사이트를 포함하여 표시시키는 등 행해지는 경우가 있다.

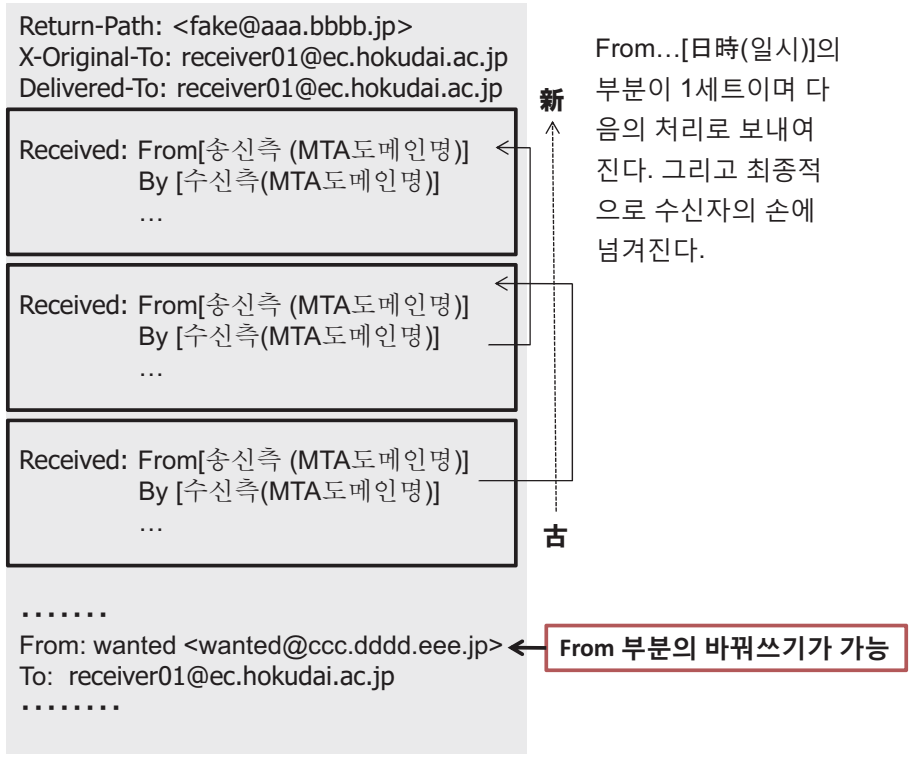
웹 사이트에의 링크 예

②A【웹 사이트로의 링크인 경우】
링크를 클릭하면 ID나 비밀번호, 신용카드 번호와 같은 정보 입력을 요구하는 화면이 표시된다. 속아서 정보를 입력하면 범인에게 정보가 송신된다.

②B【첨부 파일의 경우】
첨부 파일을 실행하면 숨어있는 트로이 목마와 같은 바이러스나 키로거 등이 실행되어 범인에게 수시로 정보를 송부한다.
최근에서는 피싱 사기의 수법도 교묘해지고 있다. 제시한 예시와 상관없이 정보를 입력하거나 신규 소프트웨어를 인스톨 할 때는 정말로 신뢰할 수 있는 것인가를 검토하고 알 수 없을 경우에는 실행하지 않는 등의 주의가 필요하다.

메일 헤더 정보

피싱 사기를 만나지 않기 위해서는 평소부터 ID나 비밀번호, 암호번호, 신용카드 번호와 같은 것을 안이하게 입력하지 않고 또한, 부주의하게 안전 한지 모르는 소프트웨어를 인스톨하지 않는 태도가 필요하다. 본고에서는 기타 많은 피싱 사기로 사용되는 메일에 대해서 보충한다. 우선 메일의 표면상 가짜 송신자로 둔갑하는 것은 용이하다. 보다 상세한 정보가 쓰여져 있는 헤더 정보의 개략은 모식적인 예(발췌)로 이하와 같다.
메일의 헤더 정보에서는 아래에서 순서대로 처리되고 있다. 보내져 온 메일의 통신 경로에 의심스러운 것이 없는지를 확인한다.



헤더 정보의 모식 예시