전자우편의 동작원리와 보안 및 스팸메일의 불법성

개인정보 불법 수집 및 판매 등 방지책 필요

김연수 연구원
한국정보보호진흥원
개인정보분쟁조정위원회

이 장에서는 E-mail의 원리와 다양한 기능 그리고 보안과의 관계를 알아보고자 한다. 우리가 가장 즐겨하면서도 정작 보안부분은 취약한 것이 바로 E-mail이다. 이메일의 원리에 대해서 살펴보고 취약한 보안부분을 점검해보는 것도 자신의 개인정보와 바이러스 및 각종 불법 메일을 방지하는 한 방법일 수 있다. 또한 다양한 유형의 바이러스형 메일의 특징을 알아보고 감염방지와 보안 등에 대한 유익한 정보가 되었으면 한다.

-편집자 주-

제 1절 E-mail 특성과 활용

I 정보 교환

인터넷을 활용하는 이유 중 많은 부분을 차지하는 것이 E-mail을 주고받으면 정보를 교환하는 것이다. E-mail 메시지는 주로 아스키파일(ASCII File) 형태의 이진데이터로 되어 있기 때문에 인코딩이 용이하다. 즉 E-mail에는 각종 그림, 음악, 동영상 등의 파일을 첨부하여 전송시킬 수 있고, E-mail을 통하여 금융거래를 할 수도 있는데 이때 코드화를 통하여 인터넷으로 전송되는 것이다. 네티즌 차원에서 E-mail 활용빈도는 정보나 데이터 등을 교류하는데 가장 많이 쓰이고 있고 오프라인의 편지를 대체하는 수단으로 발전하고 있다.

II 그룹 메일링(리스트)

특정 그룹의 사람들이 일정한 목적으로 메일을 통해 토론이나 정보를 교환할 수 있다. 그러기 위해서는 먼저 일정한 그룹 메일링을 운영하는 리스트 관리자에게 가입절차를 밟아 등록해야 한다. 그러면 메일링 리스트 데이터베이스에 구축된 E-mail로 정보를 일정주기(보통 일일단위)로 수신할 수 있다. 특히 리스트 관리자는 개인정보인 E-mail의 보안에 주의를 기울일 필요가 있고 특정 그룹의 E-mail은 외부로 유출되는 경우 위험성이 크기 때문에 기술적 관리적 조치를 취해야 한다.

III 인터넷 마케팅 수단

E-mail 마케팅이란 기업차원에서 고객의 성향을 분석하고 데이터베이스화하여 기업과 회원과의 관계를 지속적으로 유지하면서 E-mail로 판매, 홍보 및 기업 이미지 제고 등의 활용을 말한다. 따라서 초기의 E-mail 마케팅은 불특정 다수를 겨냥하여 무작위로 발송하는 방법이 대부분이었으나 최근에는 특정 개인에게 마케팅을 특화하고 기업차원에서는 폭넓은 이윤 확대를 꾀할 수 있게 되어 전자상거래 분야에서 개발진행중이다. 다만 전자우편이 상업적인 인터넷 마케팅 수단으로 자리잡기 위하여는 제공하는 정보가 가치가 있어야 한다. 한국광고업협회가 최근 'E-mail 마케팅과 소비자 태도 연구' 조사결과, 네티즌은 상업적인 E-mail이 갖춰야 할 조건으로 정보의 유용성을 꼽았으며 이어 관심분야, 정보의 다양성과 시의성, 물질적 혜택과 재미 순으로 응답하였다고 한다. E-mail 사용실태를 보면 대부분 1년 정도 E-mail을 사용해 왔으며 일주일간 평균 상업적 메일 수신 건수는 4.6건이며 개인적으로 사용하는 E-mail은 10.9건으로 집계되었다. 상업적 전자우편을 수신할 때 메일 숙독여부를 결정하는 데 영향을 미치는 요인은 '메일 제목'이었으며 '발신자 친숙도', '흥미로운 디자인' 등이 중요하다고 한다. 성별 나이 소득과 관련해서는 남자일수록, 나이가 많을수록 전반적인 광고평가가 높았으며 가구소득은 예상외로 저소득층일수록 E-mail 광고에 긍정적인 반응을 보여주었다.

제 2 절 E-mail 전송원리

E-mail 전송원리는 프로그램의 구동원리를 이해하는 것으로 갑이 을에게 E-mail을 전송하는 과정을 통해 살펴보기로 한다. 갑이 을에게 메일을 전송하기 위해서는 먼저 E-mail 전송 프로그램과 전송도구가 있어야 하고 이를 이용하여 메일을 작성하여 보내면 을은 자신의 E-mail 전송 프로그램과 전송도구로 메일을 받게 된다.

I E-mail 전송 프로그램 및 전송 도구 사용

1. E-mail 전송 프로그램(MUA : Mail User Agent 또는 mailer, reader)

E-mail 전송 프로그램으로는 크게 세 종류로 나누어 살펴볼 수 있다.

1) 메일관리 전용프로그램 사용

메일을 관리하는 전용프로그램으로는 아웃룩 익스프레스, 넷스케이프 메신저, 유도라 등이 있다.

2) 웹브라우저에 내장된 프로그램 사용

많이 알려진 웹브라우저로는 마이크로소프트사의 익스플로러, 넷스케이프 등이 있는데 이 프로그램들은 기본적으로 아웃룩, 메신저 등을 포함하고 있어 사용자들이 웹과 연동하여 E-mail을 사용하는데 편리함을 제공하기도 하지만 독점적으로 사용을 통제하게 된다. 물론 사용자에 따라서 웹브라우저는 익스플로러를 쓰고 E-mail은 네스케이프의 메신저를 사용할 수도 있지만 번거롭고 호환성도 떨어지며 프로그램이 중복되기 때문에 대부분 상호 교환 사용은 하지 않게 된다.

3)메일 전송 웹 서비스 사용

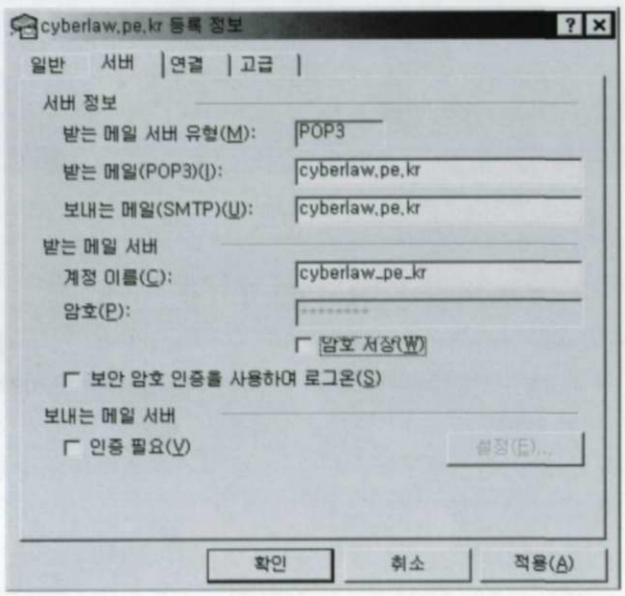
별도의 메일프로그램을 사용하지 않고 인터넷의 웹사이트

에서 메일 서비스를 하는 정보통신서비스제공자를 통하여 메일을 전수신할 수도 있다. 흔히 웹사이트에 로그인하여 자신의 E-mail을 확인하는 서비스가 이에 해당된다. 예컨대 네띠앙, 드림위즈, 한메일, 천리안, 하이텔, LETTEE 등의 서비스이다.

2. E-mail 전송 도구(MTA : Mail Transfer Agent)

POP3와 SMTP는 MTA가 사용하는 프로토콜이다.

다음의 그림은 POP3와 SMTP를 통하여 메일을 전송할 때 사용자가 기본적으로 설정해야 하는 내용이다. 즉 POP3와 SMTP라는 프토콜로 'cyberlaw.pe.kr' 이라는 서버를 통하여 'cyberlaw_pe_kr' 이라는 계정을 가진 사람의 지정된 패스워드를 확인하여 메일을 전수신한다는 의미이다.



II E-mail 작성 및 전송

갑이 메일 전송 프로그램을 통하여 '보내는 사람(갑 : pro@cyberlaw.pe.kr)', '받는 사람(을 : kimyonsu@kisa.or.kr)', '내용' 등을 기입하고 '보내기(send)'를 누른다. 메일 전수신 프로토콜은 국제규격의 기술문서(RFC : Request for comment)에 따른다. 작성된 메일은 TCP/IP 프로토콜에 의하여 패킷화(분해) 되어 내부 라우터(internal router)로 전송된다. 내부라우터는 패킷의 내용을 분석하여 내부 네트워크로 보낼 것인지, 외부 네트워크로 보낼 것인지 목적지를 결정해서 패킷을 전송한다. 외부로 전송되는 패킷은 방화벽과 게이트웨이를 거쳐 외부네트워크로 나가게 되고 몇 개의 라우터를 거쳐 상대방의 네트워크의 게이트웨이에서 패킷이 조립되어 상대방의 내부 네트워크 및 상대방의 컴퓨터에 도착하게 된다.

메일서버는 이용자의 ID와 패스워드를 검색하여 권한여부를 판별한다.

III 메일서버 도착

보내기 버튼을 누르면 메일은 cyberlaw.pe.kr 서버내 (열려있는) 일정 포트(: 데이터가 서버내 도착하는 지점 장소)에 도달한다. cyberlaw.pe.kr 서버는 'pro' 라는 계정(ID)을 사용하는 이의 메일서버로서 'pro' 가 사용하고자 하는 'pro@cyberlaw.pe.kr의 E-mail 사용여부를 인증한다.

IV 상대방의 (컴퓨터)시스템에 전송

을은 자신의 컴퓨터를 통하여 갑이 보낸 E-mail을 수신하여 열람한다.

제 3절 E-mail 관련 불법행위

E-mail의 활용은 순기능 못지않게 많은 사회적 문제를 야기한다. 정보의 교환기능을 오용하여 음란물이 전송되고, 비밀문서를 유출하며, 그룹메일링 리스트에 대한 폭탄메일 공격, 타인에 대한 무분별한 비방, E-mail 마케팅과 관련하여 스팸메일의 난무 등이 발생되고 있다. 아래에서는 E-mail과 관련된 구체적인 불법행위의 제유형을 살펴보기로 한다.

I 개인정보 불법수집

인터넷 기업들이 이용자의 개인정보를 수집하고 회원 고객관리 차원에서 대량의 리스트를 처리하게 되는데 보안이 허술한 경우 내 외부인에 의한 개인정보 유출이 용이하다. 광고 정보를 전송하는 수단으로 이용자의 개인정보, 특히 E-mail 주소를 필요로 하는데 이를 수집하는 방법은 실로 다양하다.

1. E-mail 추출 프로그램에 의한 수집

E-mail만을 수집 관리하기 위한 전문소프트웨어가 불법적으로 유통되고 있다. 일명 'E-mail 추출기' 라고도 하는데 이러한 프로그램은 자동화된 검색엔진을 가지고 PC 통신사

나 인터넷 웹사이트 게시판 등에 공개된 내용 중에서 ID와 E-mail을 수집한다. 특히 E-mail은 메시지 내용에 포함되어 있기 때문에 검색을 통하여 쉽게 찾아낼 수 있다.

프로그램으로 수집하는 방법은 먼저 통신상(게시판, 대화방 등)에서 갈무리로 수집 저장한 후 저장 파일을 프로그램에서 불러와 아이디를 검출하는데 중복되는 E-mail은 자동적으로 처리되거나 중복검색을 실시하여 단일화하여 파일로 저장한다. 다시 불러온 파일의 검출된 아이디 중 불필요한 아이디(한글, 숫자 등)는 파기하고 기본적인 ID만 추출해 다른 파일로 저장한다. 기본적인 ID만 추출된 파일을 불러들인 다음 통신사 E-mail 주소를 덧붙이기를 하여 E-mail 주소로 변환시키고 SMTP 서버에 서버명을 기재하고, 답장을 받을 E-mail 주소(허위로 기재하는 경우 발송을 제한하는 통신사도 있다), 메일을 받을 인원수, 제목, 내용 등을 기입하여 발송을 하게 된다. 수신거부메일을 받으면 해당 ID를 별도로 보관하고 차후 메일 발송시 일괄적으로 제외시키게 된다. 이 프로그램은 개당 1만원 - 1천만원대에 이르기까지 성능(수집능력, 스팸메일 발송 관리 능력 등)에 따라 천차만별이다.

2. 매매 및 암거래를 통한 수집

E-mail 마케팅이 활성화되면서 E-mail만을 대량적으로 상거래하는 사례가 늘고 있다. 인터넷 사이트의 게시판에 보면 종종 '수집된 E-mail 주소 xx개를 판매합니다' 라는 문구를 찾아 볼 수 있다. 이는 파산한 정보통신서비스제공자나 전 현직 개인정보 관리 책임자 담당자 또는 전문적으로 개인정보를 불법수집하여 관리하는 사람들이 대량의 E-mail 리스트를 판매하는데 시장에서는 직위나 보직, 인원수에 따라 별도로 가격이 책정되기도 하고 일반적으로는 1인당 50원 - 500원 정도에 거래되고 있는 실정이다.

3. 무작위 수집

아르바이트를 고용해서 인터넷에 노출된 개인정보를 수집하거나 신문, 잡지사, 공공기관 등의 공개된 E-mail을 무작위로 수집하기도 한다.

4. 기타

기타 타인의 시스템(예 : 개인의 메일 관리 프로그램)에 접근하여 불법으로 개인정보를 수집하거나 기업체의 시스템에 불법적으로 접근하여 회원 데이터베이스를 해킹, E-mail을 수집하는 경우도 있다.

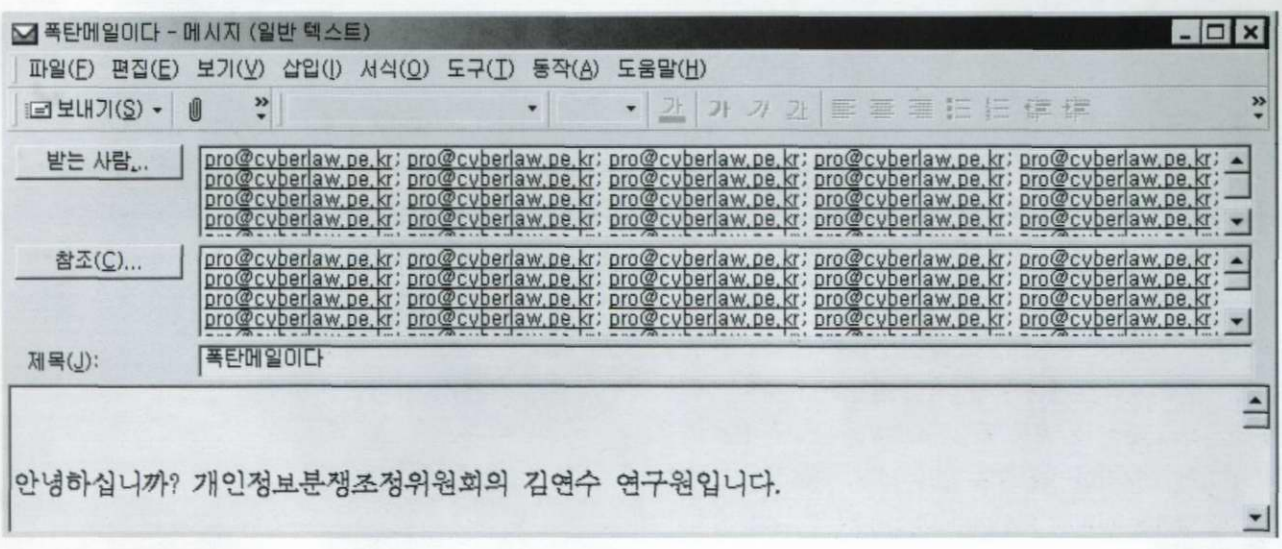
II 폭탄 메일(Bomb mail)

1. 폭탄메일의 개념

폭탄 메일은 특정인 또는 불특정인에게 할당된 메일공간에 대하여 해당 E-mail 주소로 대량의 메일을 한꺼번에 전송하는 것을 말한다. 이러한 경우 상대방의 메일서버에 과부하를 유발시키거나 개인이 중요한 메일을 수신하지 못하도록 방해할 수도 있고 심지어 시스템의 운용을 마비시킬 수도 있다.

2. 폭탄메일과 스팸메일

폭탄 메일을 특정인에 대한 메일공격으로 정의하고 광고



성 정보가 아니라는 이유에서 스팸메일과 구분하는 견해도 있으나 폭탄 메일은 스팸메일의 한 유형이다. 이는 스팸메일의 개념을 지나치게 협의로 파악하여 '수신자의 의사에 반하는 영리성 광고'에 한하여 스팸메일로 이해하려 하기 때문이다. 그러나 스팸메일은 실명 또는 비실명(예 : 허위 혹은 가명, 별명 등)으로 전자메일, 팩스, 전화 등의 전송방법을 이용해서 불필요하거나 승인되지 않은 광고, 판촉물, 금융 피라미드, 추천형식, 음란 불법 소프트웨어 복제판매, 기타 형태의 메시지를 수신자의 의사에 '관계없이'('의사에 반(反)하여'가 아니다) 일방적으로 보내는 메일이다. 법률이 처벌대상으로 하는 것은 스팸메일 중 수신자의 명백한 의사에 반하여 지속적으로 영리성 광고를 전송하는 경우에 한하고 있는 것이다. 따라서 폭탄메일은 스팸메일의 일종이라 할 수 있다.

3. 폭탄 메일의 원리

폭탄메일을 사용하는 방법은 크게 두 가지가 있는데 첫 번째는 메일 전송 프로그램(익스플로러의 아웃룩, 네스케이프 메신저 등)을 이용하는 방법이 있고 두 번째는 폭탄 메일 툴이 있어 이를 이용하는 경우이다.

1)메일 전송 프로그램을 이용하는 경우

아웃룩의 경우 '도구-계정'에서 상대방의 E-mail을 등록하게 되는데 메일환경을 설정할 때 SMTP 서버를 지정하게 된다. SMTP는 메일서버를 운영하는 업체마다 다르기 때문에 업체에 문의를 하거나 인터넷 웹사이트의 FAQ 등에서 알 수 있다(예 : 야후 메일의 경우 SMTP로 smtp.yahoo.co.kr을 쓰고, 네띠앙의 경우 netian.com을 사용한다). 일반적으로 한 명에게 한 개의 메일을 보내는 것이 원칙이지만 한꺼번에 수십 개를 동일인에게 보내도록 옵션을 지정할 수 있다. 그리고 보내는 사람을 숨길수도 있다. 즉 보내는 사람의 메일주소는 허위이거나 회신 불가인 경우가 많고, 헤더를 변경하여 발신자를 알아볼 수 없도록 하는 경우도 있다.

는 허위이거나 회신 불가인 경우가 많고, 헤더를 변경하여 발신자를 알아볼 수 없도록 하는 경우도 있다.

다음의 그림은 동일인에게 수십 개의 메일을 보낼 때 지정한 옵션 예제이다.

이러한 기초적인 폭탄메일은 보통 수십 개 정도로 전송이 되는데 용량이 작기 때문에 제한용량 미달로 간주된다. 메일 수신 프로그램에서는 보통 동일인으로부터 몇 개 이상의 동일 메일이 도착되면 이를 거부할 수 있는 기능이 있고 기업 등이 운영하는 서버나 웹서버 서비스에서는 용량을 제한하여 거부하기도 한다.

2)폭탄 메일 툴을 이용하는 경우

폭탄 메일 툴은 메일 전송 프로그램을 응용하여 소스코드를 변경해 제작된 경우가 많고 프로그램의 방식이 대체로 비슷하다. 대체로 Target(수신자), Sender(발신자), Subject(제목), Copies(전송 횟수), Contents 등으로 구성되어 있어 각 항목을 기입하고 'send'나 'Mail' 등을 누르면 옵션대로 실행된다. 공통된 사항은 메일서버(SMTP)를 통하여 폭탄메일을 보내는 것이므로 메일서버를 반드시 기입해야 한다는 점이고 메일서버는 임의의 것을 기입해도 무방하다.

4. 폭탄 메일에 대한 처벌

폭탄메일은 특정인의 시스템 운용을 방해할 목적으로 피해를 야기하기 위한 수단이므로 불법행위에 해당된다. 폭탄메일에 대하여는 정보통신망이용촉진및정보보호등에관한법률(이하 '정보통신법')과 형법에서 규율하고 있다. 관련 규정을 살펴보면 '누구든지 정보통신망의 안정적 운영을 방해할 목적으로 대량의 신호 또는 데이터를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보통신망에 장애를 발생하게 하여서는 아니 되고 이 규정을 위반하여 정보통신망에 장애를 발생하게 한 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다(정보통신법 제48조제3항 및 제62조제5호). 또한 컴퓨터 등 정보처리장치 또는 전자기록 등 특수매체기록을 손괴하거나 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하거나 기타 방법으로 정보처리에 장애를 발생하게 하여 사람의 업무를 방해한 자는 5년 이하의 징역 또는 1천5백만 원 이하의 벌금에 처한다(형법 제314조제2항).

Ⅲ 해킹툴, 컴퓨터바이러스 유포 수단

스파이웨어, 트로이목마형 해킹툴이나 컴퓨터바이러스를 유포하기 위한 방법으로 E-mail 전송을 많이 이용한다. 상대방에게는 유명프로그램의 업그레이드인 것처럼 설명하고 E-mail 메시지에 파일로 첨부하거나 아예 메시지를 열람하면 동시에 바이러스 등이 시스템에 잠입하게끔 설정한다.

(다음호에 계속)