피싱(Phishing) 피해 방지 대책

정보통신부 정보화기획실

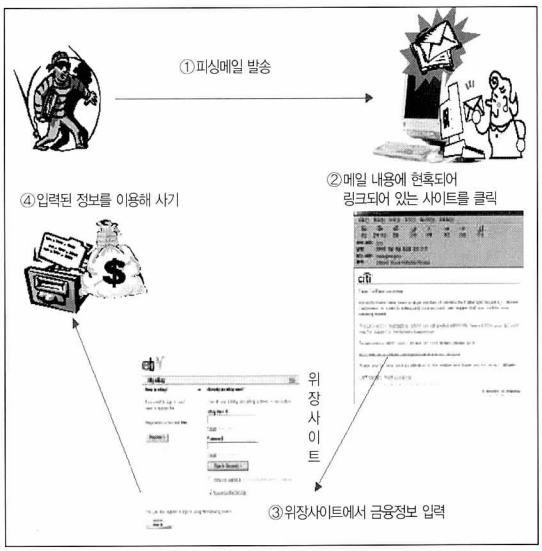
1. 피싱(Phishing) 개념

피싱(Phishing)이란 개인정보(Private Data)와 낚시(Fishing)의 합성어로 유명 업체의 위장 홈페이지를 만든 뒤, 불특정 다수 이메일 사용자에게 메일을 발송해 위장된 홈페이지로 접속하도록 현혹하여 개인정보를 빼내는 행위이다.

※ 메일 수신자의 PC에 저장되어 있는 정보를 자동으로 외부의 특정 서버로 전송하는 peep, bot류의 사고도 피싱의 한 유형으로 분류될 수 있으나, 최근의 피싱은 수신자가 현혹될 수 있는 내용의 메일을 발송하여 수신자가 직접 정보를 입력하도록 유도하는 방법으로 이루어짐

2. 피싱 발생 및 피해 실태

■ 2003년부터 대두되기 시작한 피싱은 올해 들어 급속하게 증가하여 현재까지 발견된 피싱 메일 중 92% 이상이 금년 중 발견된 것이며, 매달 평균 50%씩 증가하는 것으로 조사되었다.

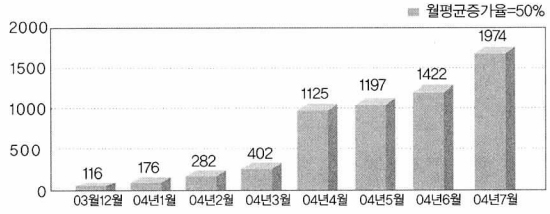


〈피싱 발생 흐름도〉

- 미국의 경우 올해 피싱메일을 수신한 사람이 5,700만명에 이르고 이 중 178만명(피싱메일수신자의 3%)이 금융정보를 제공한 것으로 조사되었으며, 영국, 독일 등도 주요 은행을 사칭한 피싱이 발생하고 있어 사회적 이슈가 되고 있는 추세

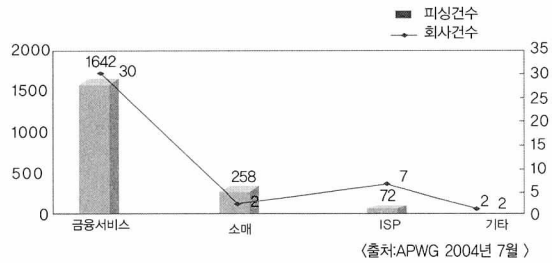
※ OECD 스팸분과 2004년 2차회의 자료에 따르면 영국

은 2003년에 한 건의 피싱도 발견되지 않았으나, 올해 상반기 동안 170만건을 수신한 것으로 보고됨



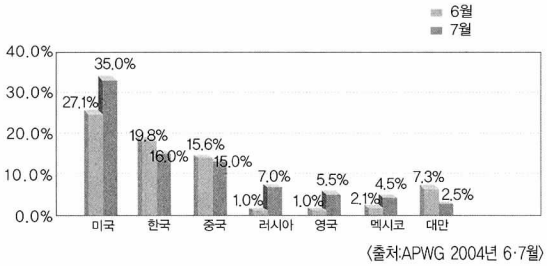
〈월별 피싱 공격 건수〉

- 전체 피싱의 80% 이상이 금융기관을 사칭하고 있으며 전자상거래 사이트가 뒤를 잇는 것으로 나타났다.



〈분야별 피싱 건수〉

■피싱 공격자는 메일 수신자를 속이기 위해 보안이 취약한 홈페이지를 해킹해 위장 홈페이지를 만들게 되는데, 주로 미국, 중국, 우리나라 등이 위장 홈페이지로 사용되어 피싱의 경유지로 이용되고 있는 상황이다



〈국가별 피싱 위장 홈페이지 호스팅 현황〉

3. 국내 피싱 실태

가. 국내에 피싱을 이용한 금융 사기 발생 우려

■우리나라의 경우 인터넷 뱅킹 등의 금융거래시 공인인증 및 안전카드를 사용하도록 되어 있어 피싱을 통해 금융정보가 유출되어도 실제 금융사기로 연계될 가능성은 외국에 비해 낮은 편이다. (아직까지 씨티뱅크, 이베이 등 외국 업체를 사칭하는 피싱이 주를 이루고 있어 영문 메일에 익숙치 않은 우리 국민의 피해는 신고되지 않고 있음) 다만, 피싱이 사회적 이슈가 됨에 따라 국내에서도 모방 범죄가 발생할 가능성이 높으며, 이 경우 정보보호 마인드가 높지 않은 우리나라 이용자들의 피해가 클 것으로 예상된다.

※ 한국정보보호진흥원의 '개인정보보호 인식 조사('02.12)' 결과에 따르면 인터넷 이용자의 94%가 개인정보침해를 우려하고 있으나, 45%만이 약관을 확인하는 것으로 나타남

나. 국내 웹사이트가 피싱 경유지로 이용

■APWG의 분석 자료에 의하면 피싱의 위장 홈페이지로(경유지)로 이용된 서버 중 우리나라의 서버가 전체의 16%를 차지하여 세계 2위를 기록했다.(2004년 7월 신고 접수된 1,974건의 피싱 중 우리나라 서버를 경유지로 한 피싱이 315건을 기록)

우리나라는 인터넷 발달과 웹호스트 서비스의 활성화로 상대적으로 많은 웹사이트가 구축·운영되고 있으나, 이에 대한 보안관리 의식은 부족해 해킹 등에 쉽게 노출되는 상황이다.

- 보안취약점을 패치하지 않거나, 서버 설정시 유의해야 할 보안 사항을 반영하지 않은 학교, 소규모 비영리단체, 중소기업 등의 웹사이트가 해킹을 당해 피싱에 이용되고 있는 것으로 조사됨

※ 2002년 5월 보안이 허술한 우리나라의 메일서버, 프락시서버가 외국 스팸머들의 스팸메일 발송 경유지로 이용되어 사회적 이슈가 된 바 있음

4. 대 책

가. 모니터링 및 신고체계 강화

■ 이메일 모니터링을 강화하여 국내에서의 피싱 발생 여부를 신속히 파악하고, 피해 확산을 조기에 차단한다.(한국정보보호진흥원에 피싱 모니터링 요원(2명)을 지정하여 상시 모니터링 실시)

■ 국민들의 피싱 신고 편의성을 제고하고 신속한 사고 처리를 위해 피싱 신고 온라인 처리 시스템을 마련(한국정보보호진흥원 홈페이지에 전담 신고 창구를 개설하고 정통부, 금융기관, 쇼핑몰, 포털사이트 등의 홈페이지에 배너로 링크)

■ 국내에서 피해가 발생할 경우 피싱 메일의 발송지 주소를 추적하여 ISP, 웹메일 사업자 등을 통해 동 메일의 수신을 차단(피싱 메일 발송자에 대하여 검 · 경에 수사 의뢰)

나. 피싱 경유지 예방 조치

■ 웹사이트를 운영하고 있으나 전문기술인력 부족으로 보안관리가 소홀한 업체 등을 대상으로 웹사이트 보안 관리 교육 실시

- KISA가 주관이 되어 다수의 웹사이트를 운영하는 웹호스팅업체, 중소기업 등 1천여개 업체 등을 대상으로 교육 실시
- 정보보호기술훈련장을 보완하여 웹사이트 관리자들에게 온라인상에서 주기적으로 신종 기술 등에 대한 교육을 받을 수 있는 서비스를 제공

■ 각급 학교의 웹사이트를 일제 점검 · 보완하도록 시도교육청을 통해 안내 공문을 발송하고 희망할 경우 각급 학교 전산관리자 교육 실시(국정원과 협의하여 학교 등 공공기관 웹사이트 보안 점검 지원을 추진)

■ 웹서버, 메일서버 등 각종 해킹의 경유지로 이용되는 주요 서버의 보안 취약점이 신속하게 패치될 수 있도록 정기적으로 관련 정보를 제공

- 웹호스팅업체, 중소기업 등에 정기적으로 보안취약점 정보를 제공하고 전담 전화 상담 창구 '중소기업 정보보호 도우미'(가칭) 개설 추진

다. 경각심 제고를 위한 대국민 홍보 · 예방 강화

■ 인터넷 이용자가 피싱의 현상과 문제점을 정확히 인식하고 적절한 대응 조치를 취할 수 있도록 '피싱 식별 및 대응 안내문을' 작성하여 관계 부처, 관련 협회 등과 공동으로 대국민 안내 활동을 전개

- 금감원, 소비자보호원 등 관련 부처에 안내문을 전달하고 소관 업체 및 국민들에게 발송하도록 협조 요청
- 인터넷기업협회, 전자상거래협회 등 주관 협회를 통해 관련 기업에 안내하고 국민들이 자주 이용하는 포털사이트 및 옥션, 인터파크 등 피싱 사기 대상이 될 수 있는 주요 인터넷 쇼핑몰 이용자에게 집중 안내
- 안내 포스터를 마련하여 대형마트, 공공기관, 대학 등 공공장소에 부착

■ 외국의 피싱 발생 사례 · 동향 등을 분석하여 국내에도 발생 개연성이 높을 시 관련 예 · 경보 발령

※ 경각심 제고를 위해 올해 5월, 7월 2차례에 걸쳐 정통부와 KISA에서 예 · 경보 발령

라. 국내 · 외 기관과 공조체계 구축

■ 미국이 중심이 된 대표적인 국제 Phishing 대응 협의체인 APWG에 회원으로 가입하여 사고정보 교환, 수사 협조 등 적극적 공조 추진

- 외국 피해 현황을 계속 모니터링하여 피싱 수법, 피해 대상 기관 등의 변화 흐름을 신속하게 파악하고 우리나라의 대응책 마련에 반영

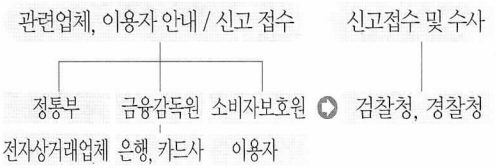
※ APWG(Anti-Phishing Working Group) : 636개 회원으로 구성되어 있으며 주로 미국 금융업체 · 전자거래업체, 호주 · 캐나다 등의 사법기관이 참여

■ 외국기관(APWG 및 미국 카네기멜론대학)과 공조하여 피

싱 기법의 변화 추세 및 기술 동향 파악

※ 오는 11월 중 미국 카네기멜론대학이 운영하는 정보보호기술연구소인 CyLab에 한국 연구소가 설립되어 한국과 미국 연구진이 공동으로 정보보호 기술을 연구

■ 피싱에 대한 정확한 국내 현황 파악 및 신속한 대응을 위해 금융감독원, 소비자보호원, 검·경찰청 등 유관기관과 상시연락체계를 마련하여 관련 동향 정보 등을 주기적으로 교환하고 소관 업체 등에게 안내 실시



〈국내 유관기관 공조체계〉

5. 추진일정

o 2004. 10 : 피싱 대응 안내문 발송·배포
o 2004. 10~ : 웹사이트 관리자 보안교육 실시
o 2004. 10~ : 피싱관련 모니터링 강화
o 2004. 11 : APWG회원 가입
o 2004. 11 : 중소기업 정보보호 전담 상담 전화 개설

피싱(Phishing) 식별 및 대응 요령

피싱이란, 개인정보(Privacy)와 낚시(Fishing)의 합성어로 유명업체(은행, 전자거래업체)의 홈페이지와 동일하게 보이는 위장 홈페이지를 만든 후, 인터넷 이용자들에게 이메일을 보내, 위장 홈페이지에 접속하여 계좌번호, 주민등록번호 등의 개인정보를 입력하도록 유인하는 신종 사기 수법을 말한다.

위장 홈페이지에 입력된 정보는 사기꾼의 손에 넘어가 각종 금융사기에 이용될 수 있다.

미국, 영국 등에서는 피싱 사기가 심각한 사회문제가 되고 있으며 우리나라에서도 모방 범죄가 발생할 우려가 있으니 인터넷 이용자들의 각별한 주의가 요구된다.

피싱 메일 식별 요령

① 유형1
- 유명 은행, 카드사 등을 사칭

※ 업체 마크, 로고 등이 메일에 포함되어 있어도 위장 사이트일 수 있음

- 계좌번호·카드번호·비밀번호 등의 확인 또는 갱신을 유도
- 확인 또는 갱신을 하지 않을 경우 거래가 중지 된다는 식의 소란을 일으키거나 자극적인 문구를 사용

② 유형2
- 포털사이트, 쇼핑몰 등을 사칭
- 경품당첨안내 또는 이벤트 참가 등을 유도하며 주민등록번호, 핸드폰 번호 등의 개인정보를 입력하도록 유도

피싱 대응 요령

① 은행, 카드사 등에 직접 전화를 걸어 이메일이 안내하는 사항이 사실인지를 확인한다.

② 이메일에 링크된 주소를 바로 클릭하지 말고, 해당 은행, 카드사 등의 홈페이지 주소를 인터넷 주소창에 직접 입력하여 접속한다.

③ 출처가 의심스러운 사이트에서 경품에 당첨되었음을 알리는 경우 직접 전화를 걸어 사실인지를 확인하고, 사실인 경우에도 가급적이면 중요한 개인정보는 제공하지 않는다.

④ 피싱이라고 의심되는 메일을 받았을 경우 해당 은행, 카드사, 쇼핑몰 및 아래 기관에 신고한다.

☞ 한국정보보호진흥원 (02)-1336 또는 (02)-118

⑤ 은행, 신용카드, 현금카드 등의 내역이 정확한지 정기적으로 확인한다.