형사정책연구 Korean Criminological Review
제20권 제4호(통권 제80호, 2009 · 겨울호)

인터넷 피싱의 형사법적 책임*

전 지 연**

국 | 문 | 요 | 약

인터넷피싱은 사기의 한 형태로서 인터넷이라는 수단을 이용하여 사기를 한다는 점에서 기존의 일반사기죄의 변형된 형태이다. 특히 우리나라의 경우 금융거래에 있어 인터넷뱅킹이 차지하는 비율이 매우 높다는 점에서 인터넷피싱의 위험성은 더욱 크다.

인터넷피싱의 다양한 유형 가운데 본고에서는 가장 전형적이고 자주 발생하는 인터넷피싱인 메일형 피싱의 형사법적 처벌가능성을 검토하였다. 특히 이와 같은 형사법적 처벌가능성은 메일형 피싱이 행하여지는 단계에 따라 검토하여 보았다.

결론적으로 인터넷 피싱 가운데 전형적인 메일피싱의 경우 피셔는 금융기관을 사칭하는 전자메일의 작성으로 사전자기록위작죄, 해당 메일을 발송하는 행위로 위작사전자기록행사죄, 메일을 발송하기 위하여 전자메일의 주소를 수집하는 과정에 전자우편주소의 무단수집죄, 위장 웹사이트 제작을 위하여 금융기관의 홈페이지를 복사한 경우 저작권법위반, 피해자가 위장 웹사이트에 개인의 금융관련 정보를 입력하여 이를 취득하는 행위는 '속이는 행위에 의한 개인정보수집 위반죄', 해당 피해자의 비밀번호 등을 이용하여 계좌를 열람하는 행위는 정보통신망법상의 무단침입죄와 비밀침해죄, 그리고 자금을 이체하는 행위는 형법상의 컴퓨터사용사기죄에 해당하는 것으로 판단하였다.

❖ 주제어 : 인터넷피싱, 신원절도, 정보통신망법, 사기, 컴퓨터사용사기

* 이 글은 한국형사정책연구원이 주최한 2009년 추계학술회의에서 발표된 내용으로 발표자가 일부 수정한 것이다.

** 연세대학교 법학전문대학원 교수, 법학박사

Ⅰ. 서

시간적 한계와 장소적 제약을 뛰어 넘어 인터넷을 통하여 필요한 자료나 정보를 검색하여 이용하고, 은행에 가는 대신에 인터넷뱅킹 등을 통하여 금융기관의 업무를 본다. 그리고 인터넷으로 쇼핑을 하고, 친구를 사귀고, 대화를 나누고, 게임을 하며 여가를 즐기기도 한다. 또한 인터넷을 이용하여 강의를 듣고 시험을 보며, 메시지를 주고받는다. 이와 같이 인터넷은 거의 모든 생활 영역에서 우리에게 편리함과 신속성이라는 매우 긍정적인 효과를 보여주었다. 그러나 인터넷의 편리함에도 불구하고 인터넷의 급속한 보급과 확대로 인하여 인터넷의 부정적인 측면이 나타나기 시작하였다. 개인적인 비밀이나 정보의 무차별적인 공개로 인한 명예나 비밀의 침해, 저장매체의 대용량으로 인한 해당 정보 유출시 피해범위의 막대함, 인터넷상에서 새로운 경제적 가치를 지니는 전자기록들(사이버머니, 아바타, 아이템 등)에 대한 침해, 새로운 업무방해형태로서 바이러스유포나 DDos공격에 의한 사이버테러형 업무방해 등 '인터넷범죄'라는 인터넷의 부정적 모습도 출현하였다.

인터넷피싱 역시 이와 같은 인터넷의 부정적 모습의 하나이다. 다른 인터넷범죄와 인터넷피싱의 차이는 다른 인터넷범죄는 인터넷에 의하여 비로소 가능하게 된 범죄이지만, 인터넷피싱은 기본적으로 사기의 한 형태로서 인터넷이라는 수단을 이용하여 사기를 한다는 점에서 기존의 일반사기의 변형된 형태에 해당한다.

피싱이라는 용어는 보통 '신원절도'(identity theft; Identitätsdiebstahl)의 변형된 형태를 의미하며, 비밀번호(password)와 낚시(fishing)가 결합된 용어라고 한다.[1] 여기서 피싱을 하는 피셔는 개인정보들 가운데 특히 인터넷뱅킹에 필요한 주민등록번호, ID, 비밀번호, 계좌번호, 인증서의 인증번호 등 금융관련 정보들을 알아낸 다음, 이를 이용하여 피해자의 계좌에서 자금을 이체하는 행위를 한다.

특히 우리나라의 경우 금융거래에 있어 인터넷뱅킹이 차지하는 비율이 매우 높은

1) Marberth-Kubicki, Computer- und Internetstrafrecht, 2005, 80면; Stuckenberg, Zur Strafbarkeit von Phishing, ZStW 2006, 877-878면; 박희영, 인터넷 금융사기(Phishing) 관련자의 형사책임에 관한 연구, 인터넷법률, 2006.10(통권 제36호), 88면. 이에 반하여 개인정보(private data)와 낚시(fishing)의 합성어로 보는 견해는 유용봉, 피싱범죄에 관한 형법적 고찰, 한국경찰연구, 제6권 제3호(2007 겨울), 278면 참조.

것으로 나타나 피싱의 위험성이 더욱 크다고 보인다. 2009. 9월말 현재 19개 금융기관(17개 국내은행, 홍콩상하이은행 및 우체국)에 등록된 인터넷뱅킹 등록고객수(동일한 고객이 2개 이상의 금융기관에 등록되어 있는 경우 중복 합산)는 5,729만명으로 2009.6월말의 5,557만명에 비해 3.1%(172만명)나 늘어난 숫자이다. 또한 2009년 9월말 현재 금융결제원의 인터넷뱅킹용 공인인증서 발급수(1인당 1개만 발급)는 1,487만개이며, 2009년 3/4분기중 인터넷뱅킹 이용 건수 및 금액(일평균 기준)은 2,903만건, 30조 1,688억원(전분기 대비 6.5%상승)에 달한다. 또한 2009.9월중 금융서비스 전달채널별 업무처리비중(건수기준)을 보면 입출금거래시 비대면거래 비중은 86.4%를 차지(CD/ATM 이용 비중이 38.0%로 가장 높았으며 이어 인터넷뱅킹이 36.2%)하였으며, 조회서비스의 비대면거래 비중은 80.1%를 기록(이중 인터넷뱅킹을 통한 조회 비중(61.8%)이 가장 높은 수준)하였다.[2)]

이하에서는 인터넷 피싱의 현재상황에 대하여 통계를 중심으로 설명하고(II), 피싱이 행하여지는 유형을 몇 가지로 나누어 살펴본다. 그리고 여기에서는 최근의 새로운 피싱 유형까지 언급될 것이다(III). 이어서 가장 많이 발생하는 인터넷피싱의 유형을 피싱이 행하여지는 단계별로 나누어 각각의 단계별 행위에 대한 형사법적 처벌가능성을 세부적으로 검토하여 본다. 여기의 형사법적 처벌에는 형법뿐만 아니라 형사특별법 특히 정보통신망이용촉진및정보보호등에관한법률(이하에서는 '정보통신망법'이라 칭한다)의 위반여부도 살펴본 후(IV), 이제까지의 논의를 요약하여 결론을 맺고자 한다(V).

Ⅱ. 인터넷피싱의 현황

1. 국제 동향

국제피싱대응 협의체인 APWG(Anti-Phishing Working Group)의 보고서에 따르면, APWG에 신고된 피싱사이트건수는 2006년 월평균 28,103건, 2007년 월평균 30,305건으로 증가추세가 이어져, 2008년 4월에 55,643건으로 가장 높은 수치를 기록

2) 한국은행, "2009년 3/4분기 국내 인터넷뱅킹서비스 이용현황"(2009년 10월 26일 공보 2009-10-27호).

한 이후, 매달 지속적으로 하락하여 2008년도 전체로는 월평균 23,200건을 나타내서 다소 감소하였다.[3)]

APWG의 2008년도 12월의 통계를 기준으로 분석하여 보면, 피싱호스트가 속한 국가별 순위에서는 전체 신고건수의 호스트비중에서 미국(55.75%), 중국(12.32%), 스웨덴(9.30%) 등이 상위에 올랐고, 한국은 3.33%(2008년 11월에는 3.09%)로 독일, 캐나다에 이어 6위에 해당되는 것으로 나타났다. 또한 입력되는 키값을 유출하는 키로거나 트로이목마, 웹서버해킹을 위한 각종 공격도구나 스크립트 등 피싱사고와 관련해 크라임웨어(crimeware)의 이용이 증가추세라고 밝혔으며, 사칭대상 기관의 유형별로는 은행, 카드사, 전자지불업체 등 금융관련 기관이 약 84%를 차지하고, 경매업체 11%, 기타 업체가 5%를 차지한 것으로 분석되었다. 주목할 만한 것은 2008년도 3분기에 전자지불업체를 사칭한 것이 24%에 달하였으나 2008년도 4분기에는 38%로 급속히 증가하여, 사칭기관의 중점이 변화하는 것이 아닌가이다.[4)]

또한 국제적 보안업체인 시만텍(Symantec)에서 '08년 11월 발표한 언더그라운드 시장의 실태 분석보고서에서도 피싱이나 DB해킹 등의 수법으로 훔친 개인의 신용정보나 해킹툴 등을 매매하는 언더그라운드 시장의 광고정보를 1년('07년 7월 - '08년 6월)간 분석해 본 결과 신용카드정보가 전체의 31%, 은행의 계좌정보가 20%를 차지하였다는 분석결과를 내놓았다.

2. 국내 동향

한국정보보호진흥원의 보고서에 의하면 2008년 한해 동안 인터넷침해사고대응지원센터(KrCERT/CC)로 접수된 '피싱경유지 사고건수'[5)]는 총 1,163건으로 집계되었다. 이는 2007년(1,095건)에 비하면 68건(6.2%)이 증가, 2006년도(1,266건)에 비해서는 103건(8.1%)이 감소된 것으로, 최근 3년 동안 증감의 변화는 크지 않았으며, 비슷한

3) APWG, Phishing Activity Trends Report, 2nd Half 2008, July-December 2008, 4면 참조.

4) APWG, Phishing Activity Trends Report, 2nd Half 2008, July-December 2008, 7면.

5) 피싱경유지 사고건수는 KISA(한국인터넷진흥원)가 국외의 침해사고대응기관이나 위장사이트의 대상이 된 기관 또는 업체, 일반사용자로부터 신고 받아 처리한 건수로써 실제 피싱으로 인한 피해사고건수가 아니라 보안이 취약한 국내시스템이 피싱사이트 경유지로서 악용되어 신고된 건수를 말한다.

수준의 통계치를 보여주고 있다.[6]

피싱경유지로 악용되는 피해를 입은 국내기관을 유형별로 분류해 보면, 중소기업 및 호스팅 업체 등이 포함되는 기업(44.8%)이 가장 큰 비중을 차지하였고, 종교단체나 비영리단체가 포함되는 비영리(9.4%), 개인홈페이지 등이 포함되는 기타/개인(8.0%), 사립대학교가 포함되는 교육(7.7%) 순으로 나타났으며, IP의 실제 사용기관을 확인할 수 없는 경우 등이 포함된 ISP서비스이용자군(30.2%)순으로 집계되었다.

2008년도 전체 사고건수를 사칭기관별로 분석해 보면, 총 24개국 124개 기관으로 '07년도(137개) 대비 13개 기관이 감소하였고, 상위 10개 기관의 사고건수가 전체사고건수의 61.4%를 차지해 사칭대상기관이 집중된 것으로 볼 수 있다.

유형별로는 은행, 전자지불업체 등 금융기관이 81.9%, 전자상거래업체가 11.1%, 그 밖에 정부기관이나 포털, 검색사이트, 미확인 등이 포함되는 기타 유형이 7.1%로 나타나, 여전히 금융기관을 사칭한 사고가 대부분을 차지하고 있음을 알 수 있다.

신고건수가 많은 상위 10개 기관에는 역시 미국, 영국, 캐나다 등 영어권국가들이, 비영어권국가로는 이탈리아, 스페인 등 유럽국가들이 해당되었다. 사칭대상기관의 소속국가별 사고건수 비중을 살펴보면, 미국이 전체건수의 61.4%로 절반 이상을 차지했고, 영국, 이탈리아, 스페인, 캐나다 등의 순으로 나타났다. 기타 국가로는 남아프리카공화국, 말레이시아, 스위스, 터키, 쿠웨이트, 자메이카 등의 다양한 국가가 포함되었다.[7]

피싱경유지 사이트 개설에 이용된 포트는 TCP/80포트가 91.8%로 대부분을 차지하였으나, TCP/84, TCP/82, TCP/8080, TCP/443 등을 포함해 총 26개의 다양한 포트가 이용되었다.

Ⅲ. 인터넷 피싱의 유형

인터넷상에서 아이디와 비밀번호, 계좌번호, 주민번호, 신용카드번호 등 개인정보를

6) 한국인터넷진흥원, 인터넷침해사고 동향 및 분석월보, 2008.12, 33면. 또한 2009년 1월부터 6월까지 피싱경유지 사고건수는 462건을 나타내고 있어, 전체적으로는 다소 감소할 것으로 전망된다(한국인터넷진흥원, 인터넷침해사고 동향 및 분석월보, 2009.06, 7면 참조).

7) 한국인터넷진흥원, 인터넷침해사고 동향 및 분석월보, 2008.12, 34면.

빼내가는 신종 수법을 가리키는 피싱은 이와 같은 개인정보를 획득하는 방법으로 다양한 수법이 사용되고 있다.[8] 이와 같은 다양한 수법 가운데 가장 많이 사용되는 피싱의 수법은 하나는 '메일을 통한 피싱'(메일형 피싱)과 다른 하나는 '악성코드유포를 통한 피싱'(악성코드유포형 피싱)의 두가지 수법이 있다.[9]

1. 메일형 피싱

메일형 피싱은 은행이나 카드사에서 보낸 것처럼 착각하게 만드는 메일을 이용하여 정보를 취득하는 피싱이다. 그리고 이러한 피싱에 많이 사용하는 사이트는 PayPal, eBay, MSN, Yahoo, Bestbuy, America Online 등이 있다고 한다.[10] 인터넷 피싱의 전통적인 수법은 금융기관의 관리자를 사칭하는 것이다. 예를 들면 "안녕하십니까. OO은행 웹사이트 관리자입니다"라고 시작되는 이메일을 은행고객들에게 보낸 후, 메일 안에서 '회원정보 수정' 등의 내용을 변경하는 것처럼 유도하여 해당란을 클릭하면 마치 진정한 해당 OO은행의 홈페이지인 것으로 위장한 사이트로 이동하여, 여기서 고객의 개인정보를 입력하게 하여, 입력한 개인정보를 빼내는 방식이다.[11]

최근에는 좀 더 지능적으로 '이벤트경품당첨' 등의 메일을 발송해 해당 부분을 클릭하면 팝업창으로 인터넷이용자의 개인적인 정보를 묻는 것처럼 유인하여 여기에 입력하는 개인정보를 빼내는 피싱도 등장했다. 또 유명 포털 사이트 게시판에 '인터넷대출' 등을 미끼로 내세워 개인정보 획득을 시도하기도 한다. 그리고 많은 경우 피셔는 국외에서 국내에 있는 자금세탁보조인을 구하여 피해자의 계좌에서 보조인 등의 계좌로 자금을 이체한 후, 다시 보조인으로 하여금 피셔가 있는 국외로 송금하게 하는 등으로 자금세탁과 범죄은닉을 하고 있다고 한다.[12]

---

8) 피싱의 진행과정에 대한 보다 상세한 설명은 Stuckenberg, Zur Strafbarkeit von Phishing, ZStW 2006, 878-880면 참조.

9) 피싱방식에 대한 상세한 설명은 유용봉, 전게논문, 279면 이하 참조.

10) Chantler/Broadhurst, Social Engineering and Crime Prevention in Cyberspace, 한국형사정책연구원 2008년 추계학술회의 발표문, 2008.11.1., 81면.

11) Walden, Computer Crimes and Digital Investigations, Oxford Uni. Press, 2007, 115-116면. 이와 거의 동일하게 진행된 미국의 AOL피싱사건에 대하여는 Chantler/Broadhurst, 전게논문, 81-82면 참조.

2. 악성코드유포형 피싱

이메일을 통해 위장사이트로 유인하여 개인정보를 획득하는 것이 주종이었던 피싱 유형이 최근에는 악성코드유포 등을 수반하는 다소 복잡하고 지능화된 유형으로 변하고 있다.[13] 미국의 세계적인 취업사이트 'Monster.com'을 대상으로 가해진 피싱·해킹 복합공격은 이를 잘 보여준다. 이 사건을 조사한 보안업체 시만텍사에 따르면, 범인은 신종 트로이목마를 사용해 Monster.com에 보관된 구직자들의 이력서에서 이메일주소와 기타 개인정보를 수집하고, 그런 다음 해당 구직자들에게 Monster.com 명의의 피싱 메일을 발송해 메일을 클릭한 구직자들의 컴퓨터를 감염시켰다. 그 피싱메일은 구직자들의 PC에 'Banker.c' 파일을 설치했다.[14] 'Banker.c'는 평범한 정보절취용 트로이목마로, 이 트로이목마는 감염된 PC를 통해 PC사용자가 인터넷뱅킹에 로그인 하는가를 감시한다. 로그인 과정이 진행되는 것을 포착하면 'Banker.c'는 사용자명과 비밀번호를 기록해 해커에게 전송한다.

Ⅳ. 인터넷피싱의 형사법적 처벌가능성

전술한 피싱의 유형 가운데 가장 전형적이고 자주 발생하는 피싱인 메일형 피싱을 중심으로 살펴본다. 메일형 피싱은 기본적으로 다음과 같은 단계를 거치며 진행된다. 첫째, 피셔는 피싱에 이용할 금융기관 명의의 전자메일을 작성하고, 위장 웹사이트를 제작하고 이를 설치하며, 보통의 경우 이러한 행위와 함께 발신할 메일주소를 수집한다. 둘째, 수집된 메일주소로 클릭하면 이미 설치해 놓은 위장 웹사이트로 링크하도록 하는 내용을 포함한 전자메일을 발송한다. 셋째, 전자메일을 수신한 예상 피해자가 해당 위장

12) Heckmann, in: jurisPK-Internetrecht, 2.Aufl., 2009, Kap.8, Rn.111.

13) 박희영, 전게논문, 89면.

14) 이 사건에서 일부 구직자들의 PC에는 'Gpcoder.e'라는 파일을 설치하게 하였다. 이 파일은 이른바 랜섬웨어(ransomware)로 인터넷사용자의 컴퓨터에 잠입해 내부문서나 스프레드시트 그림파일 등을 암호화해 열지 못하도록 만든 후 돈을 보내주면 해독용 열쇠프로그램을 전송해 주겠다며 금품을 요구하는 등의 방법으로 사용하였다고 한다.

웹사이트 주소를 클릭하고, 피해자 자신은 진정한 금융기관의 웹사이트인줄 알고 해당 사이트에 개인의 금융관련정보(계좌정보, 비밀번호, 신용카드번호, 주민등록번호 등)를 입력하고, 피셔는 이를 획득한다. 넷째, 피셔는 획득한 개인금융정보를 이용하여 피해자의 계좌나 신용카드로 자금을 이체하는 등의 행위를 하여 재산상의 이득을 취득한다.

이하에서는 이와 같은 인터넷 메일피싱에서의 해당 단계별 행위에 대하여 각각의 형사처벌 가능성을 검토하여 본다.

1. 전자메일작성과 위장 웹사이트의 제작·설치 그리고 발신 메일주소의 수집

1) 사문서위조·변조죄(형법 제231조)

피셔는 피싱에 이용할 전자메일과 여기에 첨부할 위장 웹사이트를 제작·설치함에 있어 보통 금융기관명의로 메일을 작성하고 해당 기관의 사이트를 위장한다. 문제는 여기서 전자메일을 작성하고 위장된 웹사이트를 제작한 다음 자신의 하드디스크나 특정한 서버에 저장시켜 놓는 행위가 문서에 관한 죄를 구성하는가이다. 전자메일이나 위장 웹사이트가 컴퓨터언어로 작성된 전자기록에 해당함에는 의문이 없으나, 이를 문서로써 인정할 수 있는가에 대하여는 의문이다.

문서는 사상이나 관념의 표시가 그 본질이므로 전자기록이 이러한 요소를 포함하고 있는 한에는 문서개념에 포섭될 수 있는 기본적 요건은 충족된다. 그러나 문서로 인정되기 위해서는 여기에서 더 나아가 그 표시가 가시적·가독적 부호에 의하여 표현되어야 하며, 시각적으로 볼 수 있는 것이어야 한다. 전자적으로 저장장치에 저장된 기억장치 내부의 데이터나 외부기억장치에 저장된 자료는 시각적으로 인식될 수 있는 것이 아니므로 그 자체로는 가시성이 없고, 단지 데이터의 보존기능을 가지는데 불과하다. 따라서 전자기록은 표시된 내용을 시각적 방법에 의하여 인식할 수 있는 가시성이 결여되기 때문에 문서의 개념에 포함될 수 없다.[15] 그러므로 전자메일의 작성이나 웹사이트를 제작하여 설치하는 행위를 문서에 관한 죄로 처벌하는 것은 가능하지 않다.

15) Schönke/Schröder/Cramer/Heine, StGB, 27.Aufl., 2006, §267 Rn.4; Lackner/Kühl, StGB, 25.Aufl., 2004 § 267 Rn.7; 오영근, 형법각론, 제2판(2009), 723면.

2) 사전자기록위작·변작죄(형법 제232조의2)

피셔가 제작하는 전자메일과 위장 웹사이트는 저장매체에 기록되는 전자기록에 해당하기 때문에 전자메일의 작성과 위장사이트를 제작하는 것이 사전자기록위작·변작에 해당하는가가 문제된다.

사전자기록위작·변작죄는 모든 전자기록의 위작·변작을 처벌하는 것이 아니라 사무처리를 그르치게 할 목적으로 "권리·의무 또는 사실증명에 관한 타인의 전자기록 등 특수매체기록"을 위작·변작하는 경우에 성립한다. 여기서 '권리·의무에 관한 전자기록'이란 권리·의무 또는 법률관계의 발생·존속·변경·소멸 등과 관련한 의사표시를 내용으로 하는 전자기록을 말하며, 사실증명에 관한 전자기록이란 '법률상 또는 사회생활상 중요한 사실이 표시되어있는 전자기록'[16]을 말한다.

전자메일의 경우에는 금융기관의 명의를 도용하여 금융기관시스템의 관리자인 것처럼 작성한다. 그리고 그 내용은 일반적으로 고객의 계좌번호와 비밀번호 등을 변경하여야만 한다거나, 금융정보시스템이 변경되어 다시 고객의 개인정보를 재등록하여야만 인터넷뱅킹을 이용할 수 있으며, 일정시간 동안 이를 하지 않는 경우에는 이용에 있어 불편함이 있을 수 있다는 등의 내용을 포함한다. 이와 같은 메일의 내용은 결국 고객과 금융기관간의 거래에 있어 중요한 사항에 대한 변경이나 확인을 요청하는 것이기 때문에 사전자기록에 해당하고,[17] 이를 기망하여 작성한 메일은 사전자기록위작에 해당한다.[18]

더 나아가 첨부한 위장 웹사이트 역시 '권리·의무 또는 사실증명에 관한' 전자기록인가에 대하여는 논란이 된다. 여기서 일부의 견해는 피싱을 위하여 위장 홈페이지를 제작하여 설치한 경우 해당 위장웹사이트 설치 역시 사전자기록위작죄(형법 제232조의2)가 성립하는 것으로 이해한다.[19] 그러나 이러한 해석에는 다소 문제가 있다. 위장 웹사

16) 이것은 문서에 관한 죄에서 문서는 '표시된 내용이 적어도 법률상 또는 사회생활상 중요한 사항에 관한 의사표시'이어야 한다는 판례의 입장(대판 1989.10.24, 88도1296)에 상응하는 것이다.

17) Goeckenjan, wistra 2008, 130; Heckmann, in: jurisPK-Internetrecht, 2009, Kap.8, Rn.115; Stuckenberg, Zur Strafbarkeit von Phishing, ZStW 2006, 885면.

18) 이에 반하여 전자메일의 경우 금융기관을 사칭함에 있어 해당 금융기관이 실재하지 않는 경우도 많으며, 그 내용 자체도 증명기능을 가진다고 보기 어렵다는 이유로 사전자기록성을 부정하는 입장도 있다(Graf, NStZ 2007, 131 f.).

19) Stuckenberg, Zur Strafbarkeit von Phishing, ZStW 2006, 889면; 강동범, 사이버범죄 처벌규정의 문제점과 대책, 형사정책, 제19권 제2호(2007), 44면; 박희영, 전게논문, 92면.

이트는 금융기관의 홈페이지 화면인 것처럼 가장하고 있으나 이는 권리·의무나 법률관계의 변동을 가져오는 내용은 아니다. 또한 해당 사이트 내에 중요한 사실이 표시되어 있지는 않다. 오히려 피셔에 기망당한 피해자가 해당 위장사이트나 부수된 팝업창에 자신의 개인적인 정보를 기입함으로서 비로소 사회생활상 중요한 사실이 표시되어진다. 오프라인의 경우로 말하면 공란으로 되어있는 서식에 피해자가 개인적인 사회생활상의 중요내용(성명, 주민등록번호, 주소 등)을 기입함으로써 비로소 문서로 될 수 있다. 따라서 위장 웹사이트를 제작하여 설치하는 행위를 사전자기록위작·변작죄로 처벌하기는 어렵다고 생각한다.

3) 전자우편주소의 무단 수집행위금지

메일피싱의 경우에는 피셔가 위장 사이트를 동봉한 전자메일을 보낼 사람들의 메일주소를 알아야 한다. 따라서 이를 위해 피셔는 다른 사람들의 메일주소를 수집하여야 한다. 메일주소를 수집하는 방법은 다양하나, 메일주소의 수집행위 자체가 대부분 불법한 방식이다. 즉 누구든지 인터넷 홈페이지 운영자 또는 관리자의 사전 동의 없이 인터넷 홈페이지에서 자동으로 전자우편주소를 수집하는 프로그램 그 밖의 기술적 장치를 이용하여 전자우편주소를 수집하여서는 안 된다. 또한 정보통신망법의 규정에 위반하여 수집된 전자우편주소를 판매·유통하여서도 안 된다. 더 나아가 누구든지 수집·판매 및 유통이 금지된 전자우편주소임을 알고 이를 정보전송에 이용하여서도 안 된다(정보통신망법 제50조의2). 이를 위반하여 전자우편주소를 수집·판매·유통 또는 정보전송에 이용한 자는 정보통신망법상에 의하여 처벌된다(제74조 제1항 제5호).[20] 따라서 피셔가 메일을 수집하는 과정에서 이와 같은 방법으로 수집한 경우에는 정보통신망법의 본 규정에 의하여 처벌되며, 더 나아가 메일주소를 얻는 과정에 악성코드를 사용하여 메일주소를 수집하는 경우에는 정보통신망법상의 악성프로그램유포죄(정보통신망법 제48조 제2항, 제71조)에도 해당한다.

20) 이 행위를 처벌하는 규정은 2002년 12월 정보통신망법의 개정당시에 신설된 조문으로 기본적으로는 스팸메일을 규제하기 위해 스팸메일의 발송의 전단계인 메일주소의 수집, 판매, 유통하는 행위를 처벌하려는 취지로 만든 규정이었다.

4) 저작권법위반

위장 웹사이트는 전자기록에 해당하고 이는 컴퓨터프로그램이다. 위장웹사이트는 기존의 금융기관의 사이트를 복사하여 위장사이트를 제작하므로 기존의 웹사이트에 대한 저작권의 침해가 발생할 수 있다. 진정한 금융기관 사이트는 컴퓨터 언어로 작성된 일련의 지시와 명령의 표현물이다. 따라서 저작권법 제2조 제16호의 정의규정에 따라 금융기관의 진정한 웹사이트는 '컴퓨터프로그램저작물'[21]에 해당하며, 이와 같은 컴퓨터프로그램저작물은 저작권법의 저작물로 인정된다(저작권법 제4조 제9호).[22] 따라서 이와 같은 금융기관의 홈페이지를 위장하기 위하여 동 사이트를 복제하는 행위는 저작권법 제136조 제1항의 규정[23]에 따른 저작권침해로 처벌가능하다.[24]

2. 위장웹사이트로 링크하도록 하는 메일의 발송

금융기관 명의의 전자메일을 작성하는 행위는 전술한 바와 같이 사전자기록위작죄에 해당하므로, 이와 같이 위작된 사전자기록을 고객에게 발송하는 경우 위작사전자기록행사죄(형법 제234조)에 해당할 수 있다.

여기서 전자메일의 경우 피셔가 메일을 발송하면 수신자가 가입한 인터넷서비스제공자의 서버컴퓨터 메일계정에 자동으로 입력이 된다. 따라서 수신자는 발송된 전자메일을 읽을 수 있는 상태에 있게 되므로 위작사전자기록행사죄는 성립한다.[25] 이에 반하여

---

21) 저작권법 제2조 제16호:"컴퓨터프로그램저작물"은 특정한 결과를 얻기 위하여 컴퓨터 등 정보처리능력을 가진 장치(이하 "컴퓨터"라 한다) 내에서 직접 또는 간접으로 사용되는 일련의 지시·명령으로 표현된 창작물을 말한다.

22) 이전까지는 전자기록과 같은 컴퓨터저작물들은'컴퓨터프로그램보호법'에 의하여 법적 보호가 행하여졌으나(이에 대하여는 홍승희, 정보통신범죄의 전망, 형사정책, 제19권 제1호(2007), 24-25면 참조), 2009년 4월부터는 컴퓨터프그램보호법을 폐지하고 저작권법에서 이를 보호하도록 개정하였다.

23) 저작재산권 그 밖에 이 법에 따라 보호되는 재산적 권리(제93조의 규정에 따른 권리를 제외한다)를 복제·공연·공중송신·전시·배포·대여·2차적 저작물 작성의 방법으로 침해한 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처하거나 이를 병과할 수 있다

24) 동일한 해석은 Goeckenjan, wistra 2008, 130; Heckmann, in: jurisPK-Internetrecht, 2009, Kap.8, Rn.122

25) 박희영, 전게논문, 94면.

위장 웹사이트는 증명기능을 갖추었다고 볼 수 없기 때문에 사전자기록성이 인정되지 않으므로 별개의 범죄가 성립하지 아니한다.[26]

3. 개인정보의 획득

1) 절도죄(형법 제329조)

개인정보를 획득한 피셔는 타인의 재물을 절취한 절도에 해당하는가이다. 절도죄가 성립하기 위해서는 첫째, 타인이 점유하는 타인의 재물을, 둘째, 점유자의 의사에 반하여 기존의 점유를 배제하고 자기 또는 제3자의 점유로 옮기는 절취행위를 하여야 하고, 셋째, 주관적으로 타인의 재물을 절취한다는 점에 대한 인식(고의) 뿐만 아니라 불법영득의사를 가지고 있어야 한다.

피싱을 통하여 피셔가 취득한 개인의 신용정보나 금융관련정보는 본래 피셔의 것이 아니라 피해자의 것이었으므로 타인의 것이었다. 문제는 이와 같은 개인적인 금융관련정보 등이 타인의 '재물'인가이다. 만일 이와 같은 전자적 정보들을 저장매체에 담겨져 있는 형태로 해당 저장매체를 취득하여 해당 내용들을 알았다면 저장매체에 기록된 전자정보에 대한 범죄가 아니라 해당 저장매체 자체에 범죄가 성립한다. 그러나 여기에서는 전자적 기록의 형태로 되어 있는 정보를 전자적 기록 형태로 취득하였다는 점에서 차이가 있다.

절도죄에서 '재물'의 개념에 대하여는 유체성설과 관리가능성설이 대립되고 있다. 여기서 유체성설에 의하면 외부세계에 공간을 차지하고 형태를 띠고 있는 유체물만이 재물에 해당하며, 형법 제346조를 예외규정으로 보아 관리가능성 있는 동력을 예외적으로 재물개념에 포함되는 것으로 이해한다.[27] 이것에 반해서 관리가능성설에 따르면 관리가 가능한 것이라면 유체물 뿐만 아니라 무체물도 재물에 해당하는 것으로 이해하며, 형법 제346조의 규정을 주의규정으로 파악하고 있다.[28]

---

26) 다만 피셔가 발송한 전자메일에 비밀번호 등 개인정보를 변경하지 않는 경우에는 시스템의 보안상 해당 계좌를 이용할 수 없다는 내용이 기술되어 있는 경우에는 강요죄의 가능성 있다(Heckmann, in: jurisPK-Internetrecht, 2009, Kap.8, Rn.115; Stuckenberg, Zur Strafbarkeit von Phishing, ZStW 2006, 905면).

27) 김일수/서보학, 형법각론, 2007, 274면; 박상기, 형법각론, 243면.

개인적인 금융관련 정보 등은 유체성이 결여되어 있으므로 유체물은 아니다. 물론 개인정보가 관리가능하다는 점에서는 관리가능설에 의하면 재물로 간주될 가능성이 있다. 그러나 재물에서의 관리가능은 '사무적 관리가능성'을 의미하는 것이 아니라 '물리적 관리가능성'을 의미하며, 그 대상도 관리가능한 '동력'을 의미하기 때문에 개인의 금융정보들을 사무적으로는 관리할 수 있지만 그것을 '동력'이라고 보기는 어렵다.

또한 일부의 견해에서는 재물의 개념을 목적론적 확장해석을 통해 탄력적으로 해석하여 '컴퓨터에 저장된 데이터'나 전자적 자료들을 형법상 재물로 보고자 하는 시도도 있다.[29] 그러나 이와 같은 해석은 형법의 보장적 기능을 나타내는 기본원리인 죄형법정주의, 특히 유추해석금지원칙에 반할 우려가 높은 것으로 생각되며,[30] 판례 역시 전자기록의 재물성을 부정하고 있다.[31]

따라서 피셔가 취득한 개인 신용정보들은 절도죄의 객체인 '재물'에 해당하지 아니하므로, 이를 전자적 형태로 전송받은 경우에도 절도죄로 처벌할 수는 없다.

2) 사기죄(형법 제347조)

피셔가 취득한 개인의 금융관련 정보는 재물에는 해당하지 않으나, 위장된 사이트의 이용이라는 기망의 방법에 의하여 취득한 것이므로 취득한 개인의 신용정보가 '재산상 이익'에 해당하는 경우에는 사기죄가 성립할 수 있다.

사기죄에서 '재산상 이익'은 일반적으로 재물 이외에 재산적 가치가 있는 모든 이익

28) 오영근, 형법각론, 294면; 임웅, 형법각론, 263면.

29) 하태영, 비교형사법연구, 제5권 제2호(2003), 298면 참조.

30) 상세한 논증은 전지연, 사이버범죄의 과거, 현재 그리고 미래, 형사법연구, 제19권 제3호(2007 가을), 10면 이하 참조.

31) 대법원은 "... 절도죄의 객체는 관리가능한 동력을 포함한 재물에 한한다고 할 것이고, 또 절도죄가 성립하기 위하여는 그 재물의 소유자 기타 점유자의 점유 내지 이용가능성을 배제하고, 이를 자신의 점유 하에 배타적으로 이전하는 행위가 있어야만 할 것인 바, 컴퓨터에 저장되어 있는 정보 그 자체는 유체물이라 볼 수 없고 물질성을 가진 동력도 아니므로 재물이 될 수 없다고 할 것이다...."라고 하며 전자기록의 재물성을 부정하고 있다(대판 2002.7.12, 2002도745). 또한 동일한 취지로 수수료를 받고 음란한 영상화면을 수록한 컴퓨터프로그램파일 73개를 컴퓨터통신망을 통하여 전송하는 방법으로 판매한 사건에서 컴퓨터 프로그램파일은 형법 제243조의 음란한 '물건'(기타 물건)으로 볼 수 없다고 판시하였다. 즉 전자기록으로 존재하는 화상이나 동영상들은 컴퓨터 프로그램파일형식으로 되어 있으며, 이러한 컴퓨터 프로그램파일은 음화반포죄에서 규정하고 있는 문서, 도화, 필름 기타 '물건'에 해당한다고 할 수 없다고 판단하였다(대판 1999.2.24, 98도3140).

을 의미한다.[32] 구체적으로 재산상 이익의 대상범위가 어디까지인지를 파악하려면 형법상 재산개념을 어떻게 파악하느냐에 따라 재산상 이익의 내용이 달라지기 때문에 재산개념에 관한 학설대립을 검토해 보아야 한다.

형법상 재산개념에 대하여는 기본적으로 법률적 재산설, 경제적 재산설, 법률적·경제적 재산설의 세 가지 학설이 대립하고 있다.[33] ① 법률적 재산설은 경제적 가치를 고려하지 않고 순전히 법률적으로만 재산을 파악하는 견해로서, 이에 의하면 민법상 개인이 갖는 모든 재산상의 권리와 의무가 곧 재산이다. 반면 법률적으로 승인되지 않은 불법재산이나 권리가 아닌 사실상의 이익이나 노동력은 재산에 포함되지 않는다. ② 경제적 재산설은 재산의 법률적 측면을 전혀 고려하지 않고 경제적 교환가치만을 재산의 판단기준으로 삼자는 견해이다.[34] 이에 따르면 경제적 교환가치 없는 개인의 사법상의 권리는 재산이 아닌 반면, 경제적 가치 있는 사실상의 이익과 노동력을 비롯하여 불법한 이익이라도 경제적 교환가치만 있으면 얼마든지 재산에 해당한다. 따라서 불법원인급여물에 대해서도 사기죄, 공갈죄 등이 성립하게 된다. 예컨대 매춘부의 불법한 성적 서비스도 형법상 재산상의 이익에 속하기 때문에 매춘부를 기망하여 화대를 편취한 경우에는 사기죄가 성립한다. 이 견해는 재산범죄의 재산개념을 가장 넓게 볼 수 있는 관점이며, 판례[35]의 입장이기도 하다. ③ 법률적·경제적 재산설은 경제적 교환가치 있는 재화 가운데서 법질서에 의해 승인된 것만이 재산이라고 보는 관점이다. 법질서의 통일성이라는 측면에서 다른 법률이 보호해 주지 않는 재산은 형법상의 재산으로 인정할 수 없다는 취지이다. 절충설이라고는 하지만 형법상 재산의 범위를 가장 좁게 인정하는 태도이다.

피셔가 취득한 피해자의 개인적인 금융정보는 거래계에서 유통이 금지되는 것이므로

32) Schönke/Schröder/Cramer/Perron, StGB, 27.Aufl., 2006, §263 Rn.3; 박상기, 형법각론, 305면; 오영근, 형법각론, 400-401면.

33) 전체적인 개관은 Schönke/Schröder/Cramer/Perron, StGB, §263 Rn.80 ff. 참조.

34) 이재상, 형법각론, 285면; 오영근, 형법각론, 401면; 임웅, 형법각론, 249면.

35) 대법원은 사기죄의 객체가 되는 재산상 이익이 반드시 사법상 보호되는 경제적 이익만을 의미하지 아니하고, 부녀가 금품을 받을 것을 전제로 성행위를 하는 경우 그 행위의 대가는 사기죄의 객체인 경제적 이익에 해당하므로, 부녀를 기망하여 성행위 대가의 지급을 면하는 경우 사기죄의 성립을 인정하고 있다(대판 2001.10.23, 2001도299). 또한 동일한 취지의 판례는 대판 1999.6.22. 99도1095; 대판 1987.2.10. 86도2472 참조.

이를 거래하는 것은 불법한 거래에 해당한다. 따라서 법률적 재산설이나 법률적·경제적 재산설에 의하면 개인의 금융관련정보는 재산상 이익으로 볼 수 없다. 또한 경제적 재산설에 의하는 경우에도 해당 정보는 영업비밀과 같이 그 자체가 재산적 가치를 가지고 있다고 볼 수 없다. 개인적인 금융관련 정보는 오히려 재산적 거래를 가능하게 해주는 열쇠의 역할을 하는 것이지 그 자체가 재산적 가치를 가지고 있다고 볼 수는 없다. 따라서 피셔가 취득한 개인정보를 재산상 이익으로 보아 사기죄로 처벌하는 것도 가능하지 않다.[36]

여기서 일부의 견해는 기망에 의해 비밀번호를 넘겨줌으로써 해당 계좌에 대한 재산상 처분행위를 한 것으로 볼 수 있어 사기죄가 성립한다고 본다.[37] 물론 이 경우 아직 피해자에게 직접적으로 손해가 발생한 것은 아니지만 손해와 유사한 재산상의 위험은 발생하였다는 것이다. 즉 비밀번호와 같은 개인정보의 이전으로 피해자에게 언제든지 손해가 발생할 수 있기 때문에 이는 손해에 상응한다는 것이다. 또한 사기죄에서의 재산상 처분행위는 피해자 자신이 이러한 처분행위를 인식할 필요가 없기 때문에 이미 비밀번호를 이전함으로써 사기죄는 성립한다는 것이다.

그러나 이러한 해석에는 동의할 수 없다. 피해자는 자신의 계좌에 있는 재산에 대한 처분행위 자체가 존재하지 아니하며, 또한 이를 인정한다고 할지라도 피해자의 손해는 비밀번호를 넘겨 준 행위에 의하여 직접 발생하는 것이 아니라 그것을 이용하여 계좌이체 등의 별개의 행위로 발생한다는 점에서 처분행위와 피해자의 손해 사이에 직접성도 결여되어 있다.[38] 또한 '손해발생의 위험성' 역시 재산가치의 감소가 구체적이며, 이를 피해자가 막을 수 없는 예외적인 경우에 인정될 수 있으나, 이 경우는 여기에 해당되지 아니한다. 따라서 기망에 의하여 계좌의 비밀번호 등을 이전한 행위에 대하여 금융계좌에 대한 사기죄로 처벌하기는 곤란하다.

---

36) 같은 결론은 Marberth-Kubicki, Computer- und Internetstrafrecht, 2005, 81면; 박희영, 전게논문, 96면.

37) Hilgendorf/Frank/Valerius, Computer- und Internetstrafrecht, Ein Grundriß, 2005, Rn.765; Weber, HRRS 2004, 408 f.

38) Heckmann, in: jurisPK-Internetrecht, 2009, Kap.8, Rn.116; Popp, NJW 2004, 3518; Stuckenberg, Zur Strafbarkeit von Phishing, ZStW 2006, 899면.

3) 형법상 비밀침해죄(형법 제316조 제2항)

형법은 비밀침해와 관련하여 "봉함 기타 비밀장치한 사람의 편지·문서·도화 또는 전자기록 등 특수매체기록"을 기술적 수단을 이용하여 그 내용을 알아 낸 경우를 처벌하도록 규정하고 있다(제316조 제2항). 따라서 형법상의 비밀침해죄가 성립하려면 첫째 봉함 기타 비밀장치 한 전자기록 등 특수매체기록을, 둘째 기술적 수단을 이용하여, 셋째 그 내용을 알아내야 한다[39]는 세 가지 요건이 충족되어야 한다.

피해자가 위장 웹사이트에 자신의 개인정보를 기입하여 발송함으로서 피셔가 피해자의 개인정보를 취득하는 경우 해당 개인정보는 비밀에 해당한다. 또한 웹사이트를 위장하여 개인적인 정보들을 알아냈다는 점에서 전자기록의 내용인 비밀을 취득한 것이다.

그러나 형법상의 비밀침해죄가 성립하려면 비밀을 알아낸 대상이 '비밀장치한' 전자기록 등의 비밀을 알아내야 한다. 일반적으로 정보처리시스템은 타인의 침입을 방지하기 위하여 각종 보안장치를 가동하고 패스워드 등을 입력하도록 하여 권한 있는 사람이 아니면 시스템에 접근할 수 없도록 하고 있다. 따라서 이러한 보안장치가 여기에서 말하는 '비밀장치'에 해당한다. 피싱의 경우에는 해당 비밀이 전자기록 등의 매체에 저장되어 있는 것이 아니라 피해자 자신이 직접 전자기록으로 작성하여 송부하고, 그에 대하여 다시 패스워드 등의 조치를 취하지 아니하였으므로 '비밀장치한' 전자기록에 해당하지 아니한다.[40]

또한 피셔가 개인정보를 취득한 방법 역시 '기술적 수단을 이용하여' 비밀을 알아냈다고 보기도 어렵다.[41] '기술적 수단을 이용하여 그 내용을 알아낸다'는 의미는 비밀장치한 전자기록의 내용을 알아내기 위하여 특별한 해킹프로그램을 침투시키거나, 프로

39) 여기서 '내용을 알아낸' 것과 관련하여 형법 제316조의 제1항에 규정되어 있는 일반비밀침해의 경우 비밀보호를 위한 추상적 위험범으로서 비밀장치한 편지나 문서 등의 개봉행위가 구성요건적 행위로 되어 있지만, 제2항의 경우에는 비밀을 알아내야 한다는 의미에서 침해범의 형태로 구성요건적 행위를 규정하고 있다. 따라서 편지 등을 개봉한 이상 그 내용을 알지 못한 경우에도 본죄는 기수에 이르나(통설: 박상기, 형법각론, 207면; 오영근, 형법각론, 260면; 이재상, 형법각론, 203면), 전자기록 등을 취득하였으나 아직 그 내용을 알아내지 못한 경우에는 제2항의 기수로 볼 수 없다. 다만 일부에서는 내용을 '알아냄'을 제1항의 '개봉'과 같은 의미로 해석하여 추상적 위험범으로서의 성격을 가지는 것으로 이해해야 한다는 주장(오영근, 형법각론, 261면)도 있다.

40) Heckmann, in: jurisPK-Internetrecht, Kap.8, Rn.113; .Hilgendorf/Frank/Valerius, Computer- und Internetstrafrecht, Ein Grundriß, 2005, Rn.763; Popp, MMR 2006, 85..

41) Marberth-Kubicki, Computer- und Internetstrafrecht, 2005, 81면.

그램자체의 오류를 이용하거나, 수많은 경우의 수를 자동으로 대입하여주는 별도의 프로그램 등을 이용하여 비밀장치를 해제한 후 그 내용을 알아내는 경우를 말한다.[42] 피셔의 기망에 의하여 피해자 자신이 위장사이트에 개인적인 비밀내용을 기입함으로써 피셔가 비밀을 알게 된 것을 기술적 수단을 이용하였다고 볼 수는 없기 때문에 이를 형법상의 비밀침해죄로 처벌하기는 불가능하다.

4) 정보통신망법상 비밀침해죄

정보통신망법에 의하면 누구든지 정보통신망에 의하여 처리·보관 또는 전송되는 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용 또는 누설하여서는 안 되며(정보통신망법 제49조), 이를 위반하여 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용 또는 누설한 경우에는 정보훼손죄나 비밀침해죄로 처벌하도록 규정하고 있다(동법 제71조 제11호). 형법상 비밀침해죄에서의 행위객체는 전자기록 등 특수매체기록에 저장되어 있는 비밀로 제한되기 때문에 정보통신망을 통하여 전송 중이거나 현재 처리 중인 정보를 객체로 포섭할 수 없었으나, 정보통신망법상의 비밀침해죄의 규정은 이와 같은 정보통신망을 통한 비밀침해를 처벌할 수 있도록 규정하였다.[43] 그리고 여기서 타인의 '비밀'이란 일반적으로 알려져 있지 않은 사실로서 이를 다른 사람에게 알리지 않는 것이 본인에게 이익이 있는 것을 의미한다.[44]

피셔는 위장 웹사이트를 통하여 피해자가 기입한 개인정보를 습득하였다는 점에서는 정보통신망을 통하여 비밀을 취득하였다. 그러나 이러한 비밀은 정보통신망을 통하여 처리 또는 전송되는 비밀을 취득한 것이 아니라 정보통신망을 통하여 이미 처리되었거나 전송된 피해자의 비밀을 취득한 것이다.[45] 따라서 피셔가 피해자의 개인정보를 취득

---

42) 따라서 정보시스템 관리자를 기망하여 패스워드를 알아내거나, 우연한 기회에 다른 경로를 통하여 들어서 알게 된 비밀번호 등을 이용하여 정보시스템에 침입하여 내용을 알아낸 경우에는 형법상의 비밀침해죄에서 말하는 '기술적인 수단을 이용'한 것이라고 보기는 곤란하다.

43) 더 나아가 내용을 알아내지 않고 정보를 훼손하거나 침해하는 행위는 형법의 비밀침해죄에 해당하지 않는 데 정보통신망법은 비밀을 침해하는 경우뿐만 아니라 정보 자체를 훼손하는 경우도 이를 범죄로 규정하였다(오영근, 인터넷범죄에 관한 연구, 형사정책연구, 제14권 제2호(2003 여름호), 308-309면; 홍승희, 정보통신범죄의 전망, 형사정책, 제19권 제1호(2007), 21면).

44) 동일한 취지로 대판 2006.3.24, 2005도7309; 2007.6.28, 2006도6389.

45) Goeckenjan, wistra 2009, 51; Heckmann, in: jurisPK-Internetrecht, Kap.8, Rn.114;

한 것은 비록 위장 웹사이트를 통해 비밀을 취득하기는 하였으나, 정보통신망에 의하여 처리·보관 또는 전송되는 비밀을 취득한 것은 아니므로 정보통신망법상의 비밀침해죄에 해당하지 아니한다.

5) 속이는 행위에 의한 개인정보수집 위반죄(정보통신망법)

입법자는 2008년 6월에 정보통신망법을 개정하여 누구든지 정보통신망을 통하여 속이는 행위로 다른 사람의 정보를 수집하거나, 정보를 제공하도록 유인하는 것을 금지하였으며(동법 제49조의2), 이를 위반하여 개인정보를 수집한 경우에는 처벌하도록 규정하였다(동법 제72조 제1항 제2호).[46] 이와 같은 속이는 행위에 의한 개인정보수집의 금지규정은 여기서 문제되는 메일피싱과 같은 방법으로 개인정보를 알아내는 것을 처벌하기 위하여 마련한 규정이다. 피셔는 사이트를 위장하여 피해자를 속임으로써 피해자의 개인적인 정보를 취득하였다는 점에서 인터넷 피싱의 피셔는 정보통신망법의 본 규정으로 처벌할 수 있다.

4. 획득한 개인정보를 이용한 재산상 이익의 취득

피셔는 전술한 방법으로 취득한 비밀번호와 같은 개인의 금융관련 정보를 이용하여 금융기관의 시스템에 접속하여 피해자의 계좌상황을 열람하고, 해당 피해자의 은행계좌에서 자신이나 제3자의 계좌로 자금을 이체하는 등의 행위를 하여 재산상의 이득을 취득한다. 여기서 비밀번호를 입력하여 은행의 시스템에 접속하여 피해자의 계좌를 열람하는 것은 형법상의 비밀침해죄, 정보통신망법상의 무단침입죄와 비밀침해죄의 가능성이 있으며, 피해자의 계좌에서 자금을 이체하는 행위는 컴퓨터사용사기죄의 가능성이 있다.

Hilgendorf/Frank/Valerius, Computer- und Internetstrafrecht, Ein Grundriß, 2005, Rn.762; Stuckenberg, Zur Strafbarkeit von Phishing, ZStW 2006, 883면.

46) 더 나아가 2009.4.22의 개정을 통하여 정보통신서비스 제공자는 속이는 행위에 의하여 개인정보를 수집하는 등의 사실을 발견하면 즉시 방송통신위원회나 한국인터넷진흥원에 신고하여야 하며(동법 제49조의 제2항), 방송통신위원회나 한국인터넷진흥원은 이러한 신고를 받거나 속이는 행위에 의하여 개인정보를 수집하는 사실을 알게 되는 경우에는 위반 사실에 관한 정보의 수집 · 전파, 유사 피해에 대한 예보 · 경보, 정보통신서비스 제공자에 대한 접속경로의 차단요청 등 피해 확산을 방지하기 위한 긴급조치와 같은 필요한 조치를 취하도록 규정하고 있다(동법 제49조의 제2항).

1) 정보통신망법상의 무단침입죄

보통 '단순해킹'[47]으로 불리는 정보통신망에의 무단침입을 처벌할 필요가 있는가에 대하여는 논란이 있다.[48] 이에 대하여 입법자는 "누구든지 정당한 접근권한 없이 또는 허용된 접근권한을 초과하여 정보통신망에 침입"하는 경우를 처벌하도록 규정하였으며(제72조 제1항 제1호), 더 나아가 그에 대한 미수범도 처벌하도록 규정하였다(제72조 제2항).

따라서 문제는 피셔가 피해자로부터 기망하여 얻은 비밀번호와 계좌번호 등과 같은 개인금융정보를 이용하여 금융기관의 시스템에 접속한 경우 이를 "정당한 접근권한 없이 또는 허용된 접근권한을 초과하여" 정보통신망에 침입하였는가이다.

정보통신망법상의 무단침입은 해당 정보통신망이나 시스템에 보호조치가 있는 것을 전제로 하지 아니하고,[49] 해당 통신망에 접근할 권한이 있는지의 여부에 의하여 무단침입의 여부가 결정된다. 여기서 정당한 접근권한의 존재여부를 누구를 기준으로 판단할 것인가에 대하여 해당 정보통신망을 이용하는 이용자를 기준으로 할 것인가, 아니면 정보통신망 서비스제공자(또는 관리자)를 기준으로 할 것인가에 대하여 논란이 될 수 있다.

정보통신망법상 무단침입죄를 규정하여 이를 처벌하고 있는 한에는 그 입법취지가 권한 없이 정보통신망에 침입하는 것을 막아 정보통신망 자체의 안정성과 그 정보의 신뢰성을 확보하는 것이고, 이는 이용자에 의하여 결정될 것이 아니라 정보통신망의 관리자(서비스제공자)에 의하여 결정되어야 할 것이다. 따라서 서비스제공자가 접근권

47) 해킹의 개념에 대한 유형별 설명은 이정훈, 사이버범죄에 관한 입법동향과 전망, 사이버커뮤니케이션학보, 제20호(2006), 249-252면 참조.

48) 이에 대하여는 류석준, 해킹에 대한 규제법규에 관한 연구, 비교형사법연구, 제6권 제2호(2004), 187면 이하; 류인모, 정보형법의 과제와 전망, 형사정책, 제12권 제1호(2000), 71-73면; 이상돈, 해킹의 형법적 규율방안, 법조, 2002/3(통권 546권), 112면 이하; 전지연, 사이버범죄의 과거, 현재 그리고 미래, 형사법연구, 제19권 제3호(2007 가을), 18-20면 참조.

49) 구 정보통신망법에서는 정보통신망의 보호조치를 침해하거나 훼손하는 경우를 처벌하는 규정(제29조, 정보통신망보호조치침해죄)을 두었으나, 2001년 7월 1일부터 시행된 정보통신망법에서는 이러한 보호조치 침해 규정 대신 정보통신망 침입행위 자체를 금지하는 규정을 두었다. 이것은 기술적으로 보호조치를 침해하지 아니하고 보호조치를 우회하여 정보통신망에 침입하는 경우를 포섭하기 위하여 마련한 규정으로 이해하고 있다(류석준, 전게논문, 191면; 최호진, 새로운 해킹기법과 신망된 형법적용의 흠결과 해결방안, 형사정책연구, 제18권 제4호(2007 겨울), 216면).

한을 부여하거나 허용되는 범위를 설정하고, 서비스제공자로부터 이와 같은 권한을 부여받은 이용자가 아닌 제3자가 정보통신망에 접속한 경우 그에게 접근권한이 있는지 여부는 서비스제공자가 부여한 접근권한을 기준으로 판단하여야 할 것이다.[50]

이와 같은 취지에서 대법원도 "이용자가 자신의 아이디와 비밀번호를 알려주며 사용을 승낙하여 제3자로 하여금 정보통신망을 사용하도록 한 경우라고 하더라도, 그 제3자의 사용이 이용자의 사자 내지 사실행위를 대행하는 자에 불과할 뿐 이용자의 의도에 따라 이용자의 이익을 위하여 사용되는 경우와 같이 사회통념상 이용자가 직접 사용하는 것에 불과하거나, 서비스제공자가 이용자에게 제3자로 하여금 사용할 수 있도록 승낙하는 권한을 부여하였다고 볼 수 있거나 또는 서비스제공자에게 제3자로 하여금 사용하도록 한 사정을 고지하였다면 서비스제공자도 동의하였으리라고 추인되는 경우 등을 제외하고는, 원칙적으로 그 제3자에게는 정당한 접근권한이 없다고 봄이 상당하다"[51]라고 하였다.

그러나 이와 같이 정당한 접근권한의 존부를 일방적으로 서비스제공자를 기준으로 판단하는 경우에는 이용자나 일반인에게 무단침입죄의 성립범위가 너무 확대될 위험성이 있다. 예를 들면 비밀번호의 입력과 같은 별다른 보호조치가 되어있지 않은 상태에서 단순히 "일반인은 접속하지 마십시오" 또는 "이용자는 더 이상의 내용에 대해서는 접근하지 마십시오"라는 지시가 있음에도 불구하고 접근하게 되면 권한 없는 접근에 해당한다. 또한 아이디와 비밀번호를 입력하는 등의 보호조치가 되어있는 정보통신망의 경우에도 이용권자의 동의 하에 그의 아이디와 비밀번호로 해당 통신망에 접속하는 경우도 원칙적으로 무단침입에 해당한다. 왜냐하면 대부분의 정보통신서비스제공업체는 이용자와 맺고 있는 회원계약의 약관[52]에 회원의 아이디와 비밀번호를 타인이 이용하지 못하도록 규정하고 있기 때문이다.[53]

---

50) 동일한 결론은 최호진, 전게논문, 222면.

51) 대판 2005.11.25, 2005도870.

52) 예컨대 Daum 서비스약관 제10조 제1항에는 "Daum"이 관계법령, "개인정보보호정책"에 의해서 그 책임을 지는 경우를 제외하고, 자신의 ID와 비밀번호에 관한 관리책임은 각 이용자에게 있음을 규정하고, 제2항에 이용자는 자신의 ID 및 비밀번호를 제3자에게 이용하게 해서는 안된다고 규정하고 있다.

53) 더 나아가 미수범의 경우도 처벌하므로 접속을 시도하거나 접속하기 위하여 아이디나 비밀번호를 입력해보는 행위 역시 처벌의 대상이 된다. 따라서 무단침입의 경우 미수범의 처벌규정은 삭제되어

어쨌든 메일 피싱에서 피셔의 경우에는 정당한 이용권자로부터 비밀번호와 같은 금융정보를 받기는 하였으나 이는 기망에 의하여 취득한 것이므로 이용자의 기준에서 정당한 접근권한 있는 자로 볼 수 없다. 또한 정보통신서비스제공자의 입장에서도 기망하여 비밀번호 등과 같은 정보를 취득한 피셔에게 정보통신망에 접근할 수 있는 권한을 부여하였다고 보기도 어렵다. 이러한 점에서 피셔의 경우에는 '정당한 접근권한'의 판단기준에 대하여 어떠한 기준에 의할지라도 정당한 접근권한이 있다고 볼 수 없다. 따라서 금융기관의 시스템에 접속하여 피해자의 계좌를 열람하는 등의 피셔의 행위는 정보통신망에 무단침입한 것에 해당하므로 정보통신망법상의 무단침입죄로 처벌할 수 있다.

2) 형법상의 비밀침해죄

피셔가 피해자를 기망하여 취득한 비밀번호를 입력하여 피해자 개인의 계좌를 열람하는 것은 비밀번호를 통하여 '비밀장치'되어 있는 전자기록의 내용을 알아내는 것이다. 문제는 이와 같은 전자기록의 비밀을 알아낸 것을 '기술적 수단'을 이용하여 알아내는 것인가이다.

형법상 비밀침해죄에서 '기술적 수단을 이용하여' 그 내용을 알아낸다는 의미는 비밀장치한 전자기록의 내용을 알아내기 위하여 특별한 해킹프로그램을 침투시키거나, 프로그램자체의 오류를 이용하거나, 수많은 경우의 수를 자동으로 대입하여주는 별도의 프로그램 등을 이용하여 비밀장치를 해제한 후 그 내용을 알아내는 경우를 말한다. 정보시스템 관리자를 기망하여 패스워드를 알아내거나, 우연한 기회에 다른 경로를 통하여 알게 된 비밀번호 등을 이용하여 정보시스템에 침입하여 내용을 알아낸 경우에는 여기서의 '기술적 수단을 이용'한 것이라고 보기는 곤란하다.

따라서 피해자 자신이 위장사이트에 개인적인 비밀번호 등을 기입하여 송부함으로써 피셔가 비밀번호를 알게 되고, 이러한 비밀번호를 진정한 금융기관의 사이트에 입력하여 피해자 개인의 계좌상태를 알아낸 경우에는 비밀침해죄에서의 '기술적 수단을 이용'하였다고 볼 수 없으므로, 이를 형법상의 비밀침해죄로 처벌할 수는 없다.

야 하고, 무단침입의 경우는 보호조치의 여부라는 제한이나 특정 범죄를 범할 목적이라는 주관적 요소에 의한 제한이나 어떤 방식으로든지 제한이 필요하다.

3) 정보통신망법상 비밀침해죄

정보통신망법상 비밀침해죄는 정보통신망에 의하여 처리·보관 또는 전송되는 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용 또는 누설하는 경우에 성립한다(정보통신망법 제49조, 제71조 제11호).

피셔는 피해자를 기망하여 취득한 피해자의 비밀번호나 계좌번호 등을 금융기관의 사이트에 입력함으로써 '타인의 비밀을 도용'한 것에 해당한다.

더 나아가 피셔가 비밀을 '침해'한 것인가에 대하여는 의문이다. 먼저 법문에서 사용된 '침해'라는 용어는 매우 불확실하고 모호한 개념이다. 형법상의 비밀침해죄에서는 명시적으로 '침해'라는 용어를 사용하지 않으나, 비밀침해죄의 내용상 '침해'는 기본적으로는 '비밀을 알아내는 것'이라고 이해할 수 있다. 침해의 개념을 이와 같이 이해하면 피셔는 이미 피해자의 착오로 인하여 비밀번호 등을 알았으므로, 이후에 해당 비밀번호를 입력하는 것을 '비밀의 침해'로 보기는 어렵다. 따라서 금융기관사이트에 피해자의 비밀번호를 입력하는 것은 정보통신망법상의 비밀의 '침해'에 해당하지는 아니한다.

비밀번호의 입력은 비밀의 침해가 아니지만 비밀번호의 입력을 통하여 시스템에 접속하여 피해자 개인의 계좌상태를 열람할 수 있었기 때문에, 이와 같은 피해자의 금융계좌를 열람한 것이 타인의 비밀을 침해한 것이 아닌가이다. 여기서도 전술한 바와 같이 '침해'를 '내용을 알아내는 것'이라는 의미로 이해하면, 이 경우에는 피셔는 정보통신망에 의하여 보관되는 타인의 비밀인 피해자의 계좌상태를 알아냈음으로 정보통신망법상의 비밀침해에 해당한다.[54]

따라서 이 단계에서 피셔는 비밀번호의 입력으로써 타인의 비밀을 도용하고, 피해자의 계좌를 열람함으로써 비밀을 침해하는 정보통신망법상의 두 개의 비밀침해죄를 범한 것으로 평가할 수 있다.

4) 컴퓨터사용사기죄(형법 제347조의2)

피셔가 취득한 비밀번호를 입력하여 금융기관의 시스템에 접속하여 피해자의 예금계좌에서 자기 또는 제3자의 계좌로 자금을 이체시키는 경우 어떤 범죄가 성립가능한가

54) 동일한 결론은 박희영, 전게논문, 102면.

가 문제된다.

자금의 계좌이체는 '재물'의 취득이 없다는 점에서 절도죄의 성립이 부정되고,[55] 사람에 대한 기망과 그에 따른 처분행위가 없다는 점에서 사기죄의 성립도 부정되며,[56] 피셔가 금융기관과의 관계에서 신뢰관계가 없다는 점에서 배임죄의 성립을 인정하기도 불가능하다.[57]

우리 형법은 이러한 인터넷뱅킹 등을 통해 부당하게 재산상 이득을 취득하는 것을 처벌하기 위해 '컴퓨터사용 사기죄'의 규정을 두었다. 즉 "컴퓨터 등 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하거나 권한 없이 정보를 입력·변경하여 정보처리를 하게 함으로써 재산상의 이익을 취득하거나 제3자로 하여금 취득하게 한"(형법 제347조의2)[58]경우를 처벌하고 있다.

여기서 허위의 정보를 입력은 '입력조작'을 의미하며, 객관적 진실에 반하는 내용의 정보를 입력하는 것을 말한다.[59] 그리고 부정한 명령을 입력한다는 것은 소위 '프로그램조작'을 의미하며, 당해 시스템의 사무처리 목적에 비추어 주어서는 안 되는 명령을 입력하는 것을 말하고,[60] 권한 없이 정보를 입력·변경한다는 것은 권한 없이 시스템에 접속하여 부정하게 프로그램이나 데이터를 변경·조작하는 것을 말한다.

피셔가 피해자의 비밀번호를 입력하여 자금을 이체하도록 입력하는 행위는 '허위의 정보'나 '부정한 명령'을 입력하는 것이라고 보기는 어렵다.[61] 그러나 피셔는 사취한 비밀번호를 입력하였으며, 또한 진정한 예금의 소유권자가 아님에도 불구하고 해당 계

55) 이를 절도죄로 인정하는 것은 재물의 개념을 확대하는 것으로 허용되지 않으며 결과적으로 이익절도를 인정하는 것이 되어 타당하지 않다.

56) Stuckenberg, Zur Strafbarkeit von Phishing, ZStW 2006, 905면.

57) 홍승희, 정보통신범죄의 전망, 형사정책, 제19권 제1호(2007), 18면.

58) 컴퓨터사용 사기죄의 입법과정에 대해서는 오병두, 컴퓨터사용사기죄의 입법경과와 입법자의 의사, 형사법연구, 제19권 제1호(2007 봄), 109-126면 참조.

59) 형법개정법률안 제안이유서에 의하면 허위의 정보입력을 "예컨대 허위의 입금데이터를 입력하여 예금원장파일의 잔고를 증액시킨 경우와 같이 사실관계와 일치하지 않는 자료를 입력하는 경우"(법무부, 형법개정법률안 제안이유서, 1992, 182면)라고 설명하고 있다.

60) 예를 들면 "프로그램을 조작하여 예금을 인출해도 잔액이 감소되지 않게 하는 것"(법무부, 형법개정법률안 제안이유서, 1992, 182면)이 여기에 해당한다.

61) 판례는 권한 없는 자에 의한 명령입력행위를 '명령을 부정하게 입력하는 행위' 또는 '부정한 명령을 입력하는 행위'에 포함된다고 해석하고 있다(대판 2003.1.10, 2002도2363). 이에 대한 적절한 비판은 유용봉, 전게논문, 286-287면.

좌의 자금을 다른 계좌로 이체시키는 행위를 함으로써 '권한 없이 정보를 입력'한 것에 해당한다.[62] 또한 이를 통하여 재산상의 이익을 취득하였으므로 피셔의 행위는 컴퓨터 사용 사기죄에 해당한다.[63]

Ⅴ. 결어

인터넷의 부정적 모습의 하나인 피싱은 사기의 한 형태로서 인터넷이라는 수단을 이용하여 사기를 한다는 점에서 기존의 일반사기의 변형된 형태에 해당한다. 특히 우리나라의 경우 금융거래에 있어 인터넷뱅킹의 비율이 매우 높다는 점에서 인터넷피싱의 위험성은 더욱 크다고 생각된다.

매우 다양한 피싱의 유형 가운데 본고에서는 가장 전형적이고 자주 발생하는 피싱인 메일형 피싱의 형사법적 처벌가능성을 검토하였다. 특히 이와 같은 형사법적 처벌가능성은 메일형 피싱이 행하여지는 단계에 따라 검토하여 본 결과 다음과 같은 결론에 이르렀다.

첫째, 피셔가 피싱에 이용할 전자메일을 작성하고 여기에 첨부할 위장사이트를 제작·설치하며, 발신할 메일주소를 수집한다. 여기서 전자메일의 작성과 금융기관을 위장하는 사이트의 제작·설치는 해당 전자기록의 문서성(가시성과 가독성)을 인정할 수 없으므로 사문서위조·변조죄로 처벌하기는 곤란하다. 또한 해당 위장사이트가 전자기록에는 해당하지만 증명적 기능을 수행한다고 보기 어렵기 때문에 사전자기록위작·변작죄에 해당하지 않는다. 그러나 금융기관을 사칭하는 전자메일의 경우에는 고객과 금융기관 사이의 법적 거래에 중요한 의미를 지니는 내용이 포함된 전자기록이므로 사전자기록위작죄에 해당한다. 그리고 위장 웹사이트는 일반적으로 기존의 금융기관의 홈페이지를 복사하여 위장 사이트를 제작하므로 홈페이지를 복제하는 행위는 저작권법 제136조 제1항의 규정에 따른 저작권침해로 처벌가능하다. 그리고 피셔가 메일주소를 수집하는 과정에서 홈페이지 운영자 또는 관리자의 사전 동의 없이 인터넷 홈페이지에서 자동

62) Tröndle/Fischer, 54.Aufl., 2007, § 263a Rn.11.

63) Marberth-Kubicki, Computer- und Internetstrafrecht, 2005, 80면.

으로 전자우편주소를 수집한 경우에는 정보통신망법의 전자우편주소의 무단수집죄로 처벌되며, 더 나아가 메일주소를 얻는 과정에 악성코드를 사용하여 메일주소를 수집하는 경우에는 정보통신망법상의 악성프로그램유포죄에도 해당한다.

둘째, 위장 웹사이트로 링크하도록 하는 내용을 포함한 전자메일을 발송하는 행위는 위작사전자기록행사죄에 해당하고, 첨부한 위장 웹사이트의 발송에 대하여는 별도로 범죄가 성립한다고 볼 수는 없다.

셋째, 피해자가 위장 웹사이트를 클릭한 후 개인의 금융관련 정보를 입력하고 피셔는 이를 획득한다. 여기서 피셔가 취득하는 개인금융정보는 전자기록으로 재물에 해당하지 않기 때문에 절도죄의 성립은 부정된다. 또한 개인금융정보가 거래계에서 경제적 교환가치를 가지고 있다고 볼 수 없고, 그 자체의 거래가 불법한 것이므로 개인금융정보는 재산상 이익으로 볼 수도 없기 때문에 기망으로 이를 취득한 것은 사기죄에도 해당하지 아니한다. 피셔의 기망에 의하여 피해자 자신이 위장 사이트에 개인적인 비밀내용을 기입함으로써 피셔가 비밀을 알게 된 것을 형법상의 비밀침해죄에서 말하는 '기술적 수단을 이용'하였다고 이해하기도 곤란하다. 또한 정보통신망에 의하여 처리 또는 보관되는 비밀을 취득한 것이 아니라 정보통신망을 통하여 이미 처리되었거나 전송된 피해자의 비밀을 취득한 것이므로 정보통신망법상의 비밀침해죄에도 해당하지 아니한다. 다만 이 행위는 정보통신망법에 새로이 규정된 '속이는 행위에 의한 개인정보수집위반죄'에 해당할 것이다.

넷째, 피셔는 비밀번호와 같은 개인금융정보를 이용하여 피해자의 계좌에서 자금을 이체하는 등의 행위를 하여 재산상 이득을 취득한다. 여기서 피해자의 비밀번호를 입력하여 금융기관의 시스템에 접속하는 행위는 정당한 권한 없이 정보통신망에 침입한 것으로 정보통신망법상의 무단침입죄에 해당한다. 그리고 금융기관의 시스템에 접속하여 피해자의 계좌를 열람하는 것은 '기술적 수단을 이용'하였다고 볼 수 없으므로 형법상의 비밀침해죄에는 해당하지 않는다. 그러나 비밀번호의 입력으로써 정보통신망법상의 타인의 비밀을 도용하고, 피해자의 계좌를 열람함으로써 정보통신망에 보관되는 비밀을 침해하는 정보통신망법의 비밀침해죄에 해당한다. 피해자의 계좌에서 자기나 제3자의 계좌로 자금을 이체하는 행위는 기존의 재산범죄로 포섭하기는 불가능하고, '권한 없이 정보를 입력'하여 재산상의 이익을 취득하였으므로 컴퓨터사용사기죄에 해당한다.

결론적으로 인터넷 피싱 가운데 전형적인 메일피싱의 경우 피셔는 금융기관을 사칭하는 전자메일의 작성으로 사전자기록위작죄, 해당 메일을 발송하는 행위로 위작사전자기록행사죄, 메일을 발송하기 위하여 전자메일의 주소를 수집하는 과정에 전자우편주소의 무단수집죄, 위장 웹 사이트 제작을 위하여 금융기관의 홈페이지를 복사한 경우 저작권법위반, 피해자가 위장 웹사이트에 개인의 금융관련 정보를 입력하여 이를 취득하는 행위는 '속이는 행위에 의한 개인정보수집 위반죄', 해당 피해자의 비밀번호 등을 이용하여 계좌를 열람하는 행위는 정보통신망법상의 무단침입죄와 비밀침해죄, 그리고 자금을 이체하는 행위는 형법상의 컴퓨터사용사기죄에 해당한다.

Die Strafrechtliche Verantwortung der 'Internet-phishing'

Jun, Ji-Yun*

Beim Phishing (vermutlich von 'password fishing' abgeleitet) versucht der Täter mit Hilfe nachgemachter Bank-E-Mails, Bankkunden auf eine ebenfalls nachgemachte Bank-Website zu locken, um sie dort zu veranlassen, PIN und TAN einzugeben. Mit ihrer Hilfe wird dann das betreffende Konto leergeräumt.

Dies soll nach einer Ansicht durch die Möglichkeit der Abbuchung des Geldbetrages ohne die weitere Mitwirkung des Opfers die konjrete Vermögensverfügung darstellen, so daß der Betrugstatbestand mit der bewußten Bekanntgabe der Online-Banking Zugangsdaten der Betrug vollendet sei.

Solche ist jedoch über die Verfügung des Opfers sehr problematisch. Der Vetrugstatbestand ist wegen der Verfügungshandlung des Opfers nicht erfüllt. In dieser Situation führt das Opfer nicht den Vermögensverfügungshandlung, sondern nur Übergabehandlung der eigenen Password. Danach ist kein Betrug vorausgesetzt. Nach dem Übergabe der Password hat der Täter den Computerbetrugtatbestand durch die unbefugte Verwendung der fremden Password in der Online-Banking System erfüllt.

Danch ist der Phishher wegen des Computerbetruges strafbar gemacht.

❖ Key words : Internetphishing, Identitätsdiebstahl, ITcrime, Betrug, Computerbetrug

투고일 : 2009. 10. 7 / 심사(수정)일 : 2009. 11. 14 / 게재확정일 : 2009. 11. 26

* Prof., Dr.iur. an der Yonsei Law School