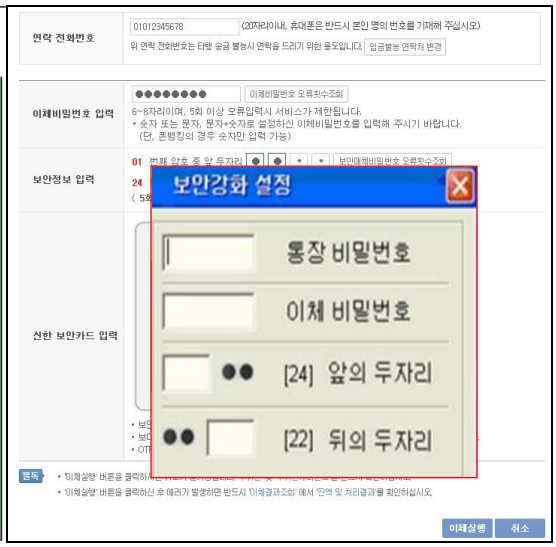
인터넷뱅킹 악성코드 감염 시 치료방법

최근들어 인터넷접속을 통해 PC에 악성코드가 감염되어, 인터넷뱅킹 거래가 정상적으로 이루어지지 않은 사례가 발생하고 있습니다. **고객님의 PC에 다음과 같은 사례가 발생 될 경우, 악성코드에 감염된 가능성이 많으므로, 당행 고객센터 신고(1577-8000) 및 악성코드 치료 후 거래하시기 바랍니다. 아래 방법으로 악성코드 치료 후에도 동일한 증상이 발생하면 PC A/S를 받아보시길 바랍니다.**

PC 신종악성코드 감염사례

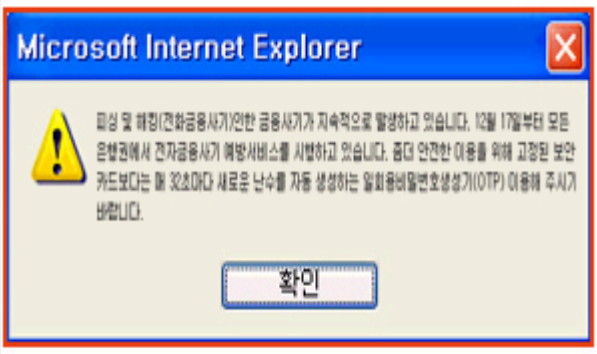
① 이체완료 단계 인증서 암호입력 시 등 거래 도중 멈춤 현상 발생 (신종)

② 보안강화 등을 이유로 보안카드 일부 팝업창으로 입력요구 (신종)



③ 보안카드 번호 전체 입력요구

④금융사기 안내 후 개인정보 입력유도



■ 거래 멈춤현상 등 신종 악성코드 감염 시 업무절차 (상기 ①②번 감염사례 경우)

- 결제를 위한 정보입력 후 멈춤 혹은 정보입력창이 특징임

① 이체완료 단계 인증서 암호입력 시 등 거래 도중 멈춤 현상 발생 (신종)

② 보안강화 등을 이유로 보안카드 일부 팝업창으로 입력요구 (신종)

-특히, 보안카드 번호 입력 진행까지 마친 경우 즉시 고객센터(1577-8000) 연락하여 보안카드 분실신고 및 계좌 지급정지 신청하시기 바랍니다.

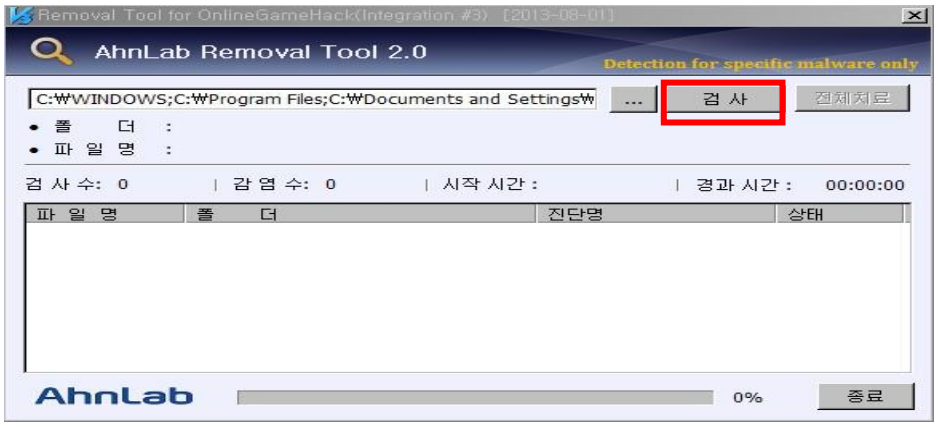
-이후 PC 악성코드 치료, 가까운 영업점을 방문하셔서 OTP 등 보안카드 재발급 인터넷뱅킹에서 전자금융사기예방서비스 가입(뱅킹보안센터 메뉴) 하시기 바랍니다.

▶ 악성코드 치료절차

- 전용 백신을 통해 정밀검사 (http://www.ahnlab.com)

1) 전용 백신 설치(다운로드 > 무료제공파일 > gamehackkill.exe)

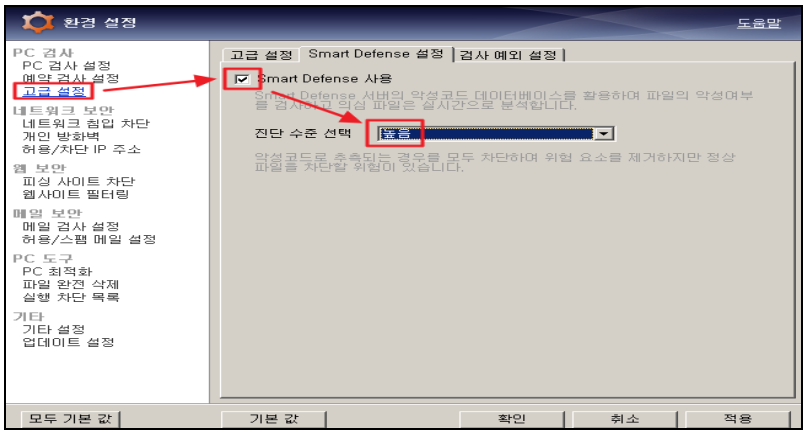
2) 전용백신을 통한 악성코드 탐지 및 치료(검사 진행)



※ 검사 완료 후 '전체 치료' 클릭 시 '재부팅 후 검사 재진행 메시지'가 나오면 '확인'을 누르고, 재부팅 및 재검사를 통해 잔재하는 악성코드를 치료 바랍니다. (재부팅 전 저장 및 확인이 필요한 부분이 있으면 반드시 먼저 처리 바랍니다)

3) V3실행 → 엔진 업데이트 버튼 클릭 (우측 하단)

4) 고급설정 → Smart Defense 사용 (체크) → 진단수준 선택 : 높음



5) 정밀검사 버튼 클릭 (검사진행)

■ 보안카드번호 전체 입력요구 악성코드 감염 시 업무절차 (상기 ③④번 감염사례 경우)

'③ 보안카드 번호 전체, ④금융사기 안내 후 개인정보 입력유도' 가 특징임

-특히, 보안카드 번호 입력 진행까지 마친 경우 즉시 고객센터(1577-8000) 연락하여 보안카드 분실신고 및 계좌 지급정지 신청하시기 바랍니다.

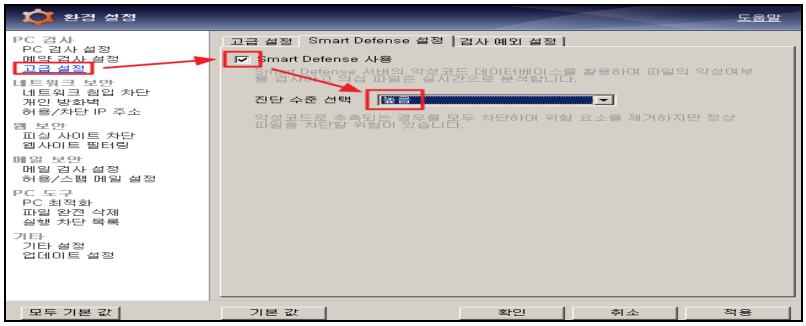
-이후 PC 악성코드 치료, 가까운 영업점을 방문하셔서 OTP 등 보안카드 재발급 인터넷뱅킹에서 전자금융사기예방서비스 가입(뱅킹보안센터 메뉴) 하시기 바랍니다.

▶ 악성코드 치료절차

- 개인용 무료 백신인 V3 Lite, 알약 등을 통해 정밀검사

1) V3실행 → 엔진 업데이트 버튼 클릭 (우측 하단)

2) 고급설정 → Smart Defense 사용 (체크) → 진단수준 선택 : 높음

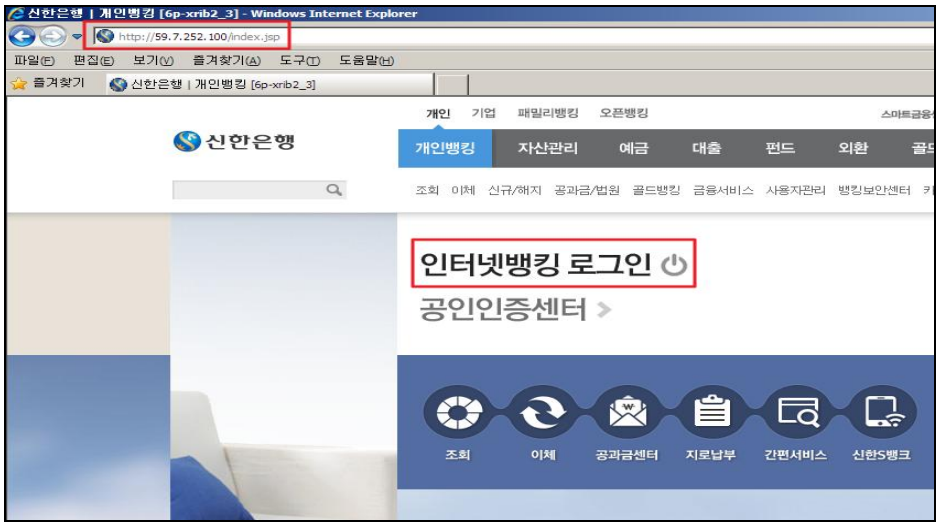


3) 정밀검사 버튼 클릭 (검사진행)

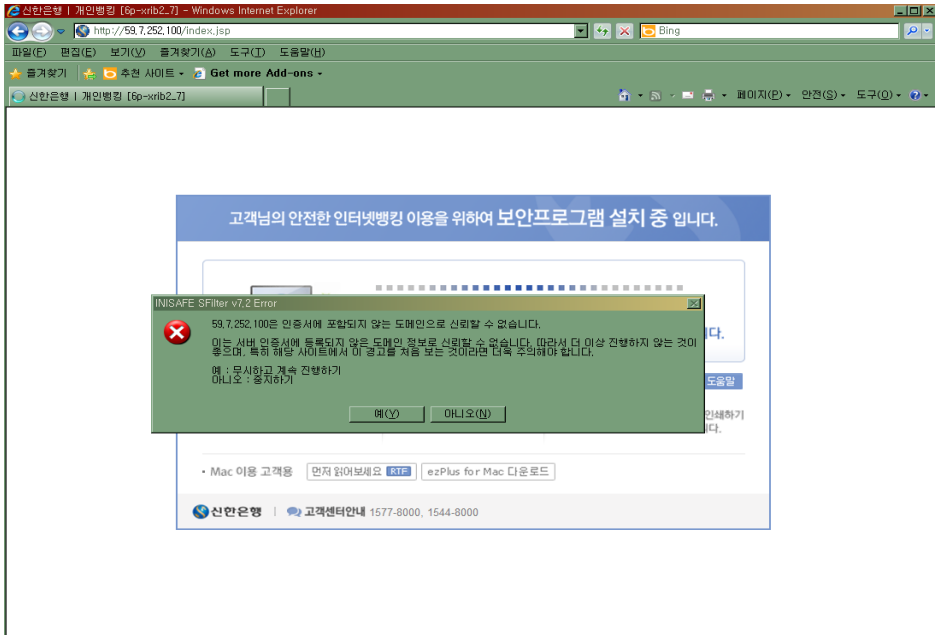
▶ 만약, 악성코드로 인해 백신 프로그램이 실행되지 않는 경우 아래절차 진행 (선택조작)
-인터넷뱅킹 홈페이지 AOS(Ahnlab Online Security) 를 통해서 검사진행

1) 인터넷 주소창에 http://59.7.252.100 입력 (신한은행 홈페이지)

2) 인터넷뱅킹 로그인 버튼 클릭

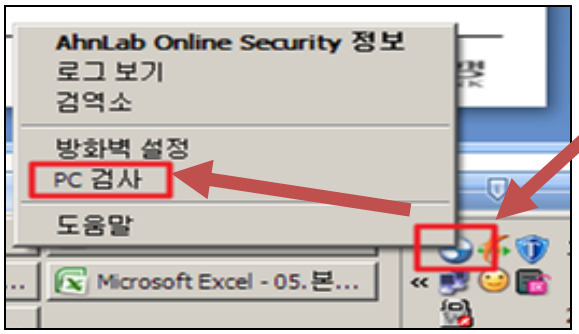


3) 아래 메시지가 표시될 경우 '예(Y)' 를 선택 → 보안프로그램 설치

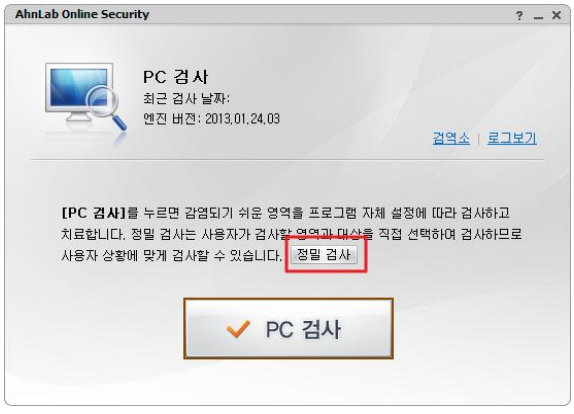


4) 악성코드 검사 (Ahnlab Online Security) 아이콘 클릭 (우측 하단에 있음, 공모양)

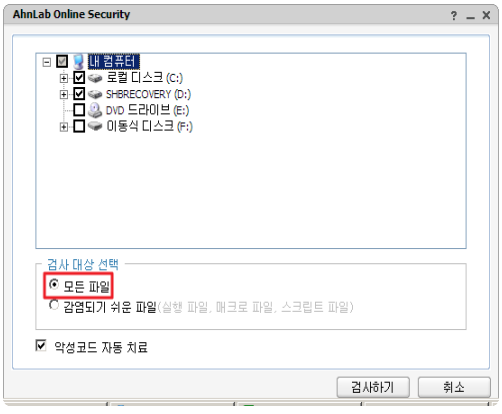
5) PC검사 메뉴 선택



6) 정밀검사 클릭



7) 모든파일 선택 → 검사하기



▶ **PC의 hosts 파일 복구조치**

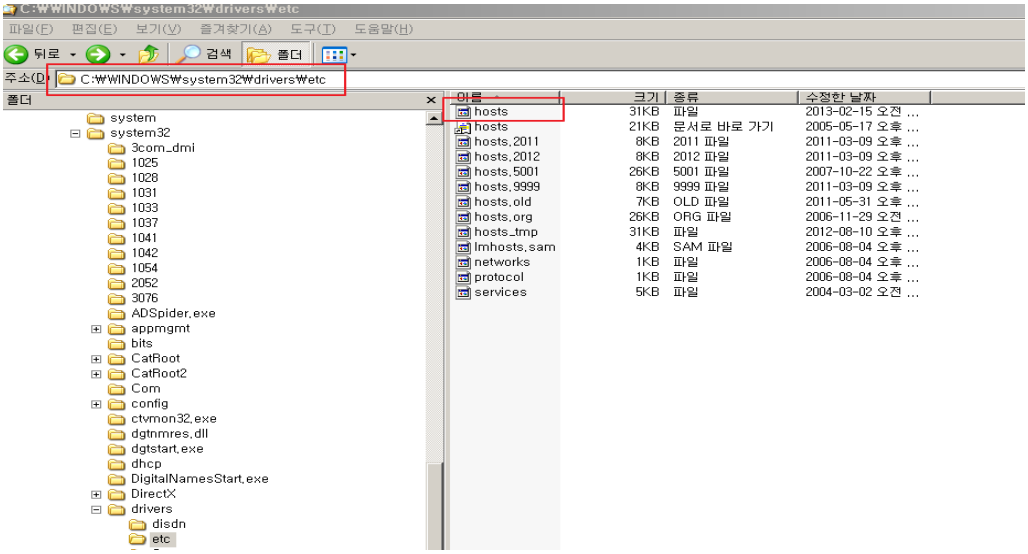
-사기 홈페이지 악성코드는 윈도우 hosts 파일을 변조하므로, 이 파일을 원상복구 조치

1) 이메일을 통해 사기사이트 IP 차단 신고 (선택사항이나 가능한 처리 부탁)

-신고내용 : 추가 피해확산을 방지하기 위해 사기사이트 차단신고

-신고방법 : pc의 hosts파일을 shbcert@shinhan.com e-mail 주소로 첨부하여 발송함

디렉토리 위치 c:₩windows₩system32₩drivers₩etc 첨부파일 : hosts 파일



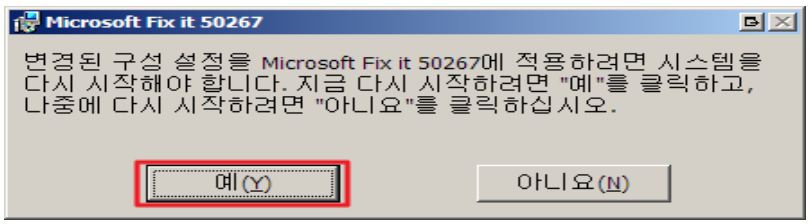
2) 인터넷 주소창에 http://support.microsoft.com/kb/972034/ko 입력

-Microsoft사 hosts 파일 초기화 사이트 접속하여 처리함

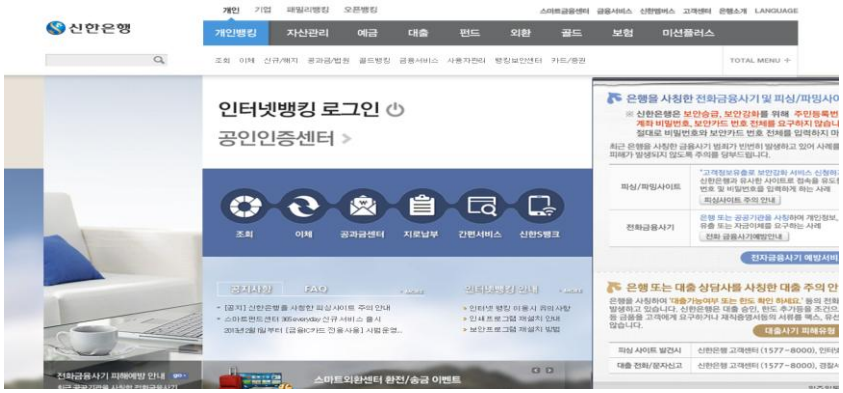
hosts파일이 초기화 되므로, 별도 설정한 값이 있을 경우 주의 (전문가용 PC 등)

3) 마우스를 아래로 내려서 hosts 파일 복구 프로그램 다운로드 (Fix it 버튼)

4) 다운받은 프로그램을 실행 → ⑤ 종료 후 PC를 재부팅 함



5) 신한은행 인터넷뱅킹 정상 사이트 접속 확인 (banking.shinhan.com)



▶인터넷뱅킹 접속 후 보안승급 강화이유로 개인정보 상세 입력이나 보안카드번호 전체 요구 등 화면이 더 이상 나오지 않아야 합니다.

▶ 인터넷뱅킹 악성코드 감염 예방법

- 백신 프로그램의 자동 업데이트를 설정
- 잘 모르는 웹사이트는 접속하지 않음
- 정품 소프트웨어를 사용
- 출처가 불분명한 파일은 다운로드하지 않음
- 이메일 첨부파일 열기 전, 인터넷뱅킹 이용 전 악성코드 검사 (V3나 알약 등)
- 이메일을 통해 전달된 링크는 직접 클릭하지 말고 주소창에 직접입력해서 확인

▶ 인터넷뱅킹 금융사기 방지안내

- 은행에서는 절대 보안승급을 요청하지 않음. 계좌번호, 비밀번호, 보안카드 번호 전체를 요구하면 바로 고객센터에 신고함
- 서비스 이용 시 의심스러운 부분이 있으면 고객센터에 확인
- 만약 개인 금융정보가 유출되었다면 즉시 고객센터에 계좌 지급정지, 보안카드 분실신고