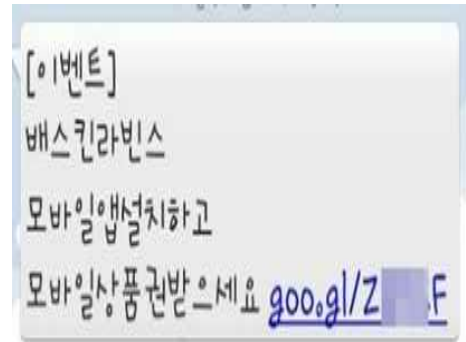
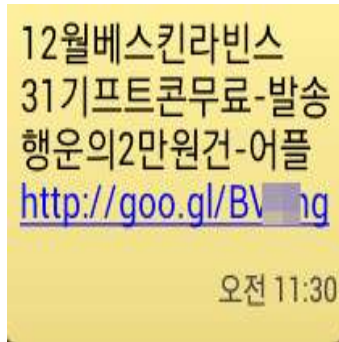
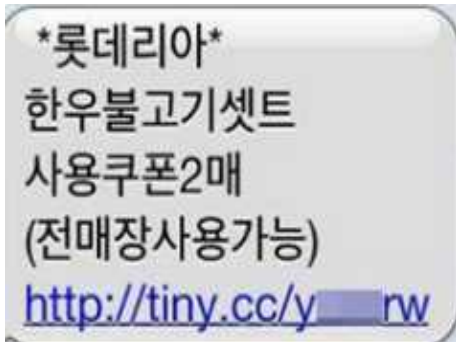


경찰청 사이버테러대응센터에서 긴급히 알려드립니다.

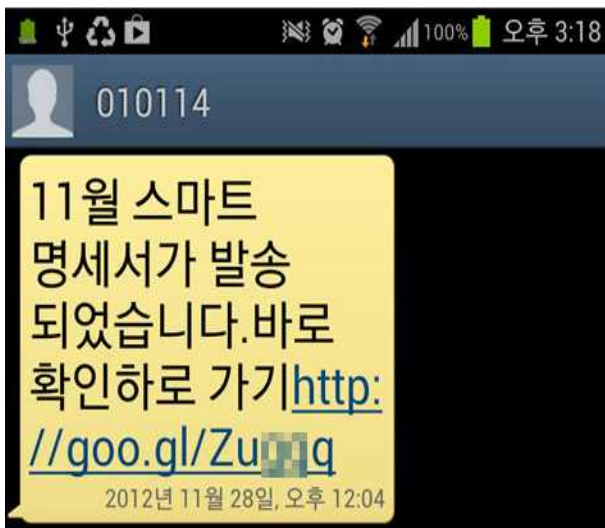
‘무료쿠폰 제공’, ‘모바일상품권 도착’, ‘스마트명세서 발송’ 등의 문자를 받아본 적이 있으시지요.

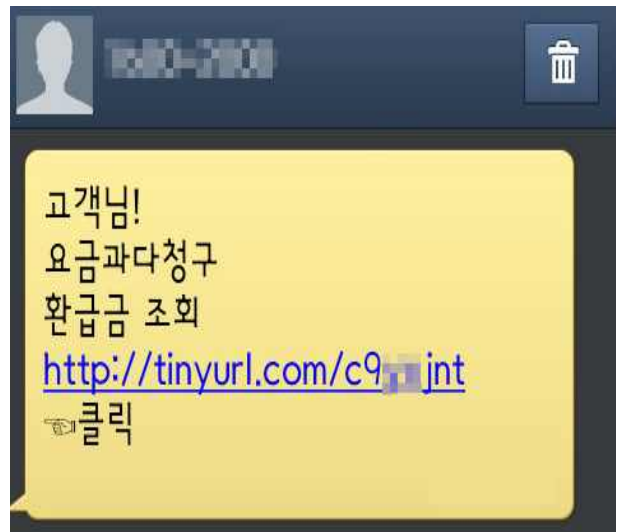


무심코 문자메시지에 기재된 인터넷주소를 누르면 한 달 후 내가 모르는 소액결제이용료가 부과되는 피해를 입을 수 있습니다.

특히 최근에는 앞서 보여드린 문자들보다 그 내용이 더 다양하고 쉽게 믿을 수 있도록 수법이 지능화되고 있어 누구나 쉽게 피해에 노출될 수 있다는 점입니다.

※ 스미싱범죄에 사용된 문자메시지





‘스미싱’ 피해 단계

- ▶ 피해자가 문자메시지내 인터넷주소 클릭 → 스마트폰에 악성코드 설치 → 범인에게 소액결제 인증번호 전송 → 범죄자는 게임아이템이나 사이버머니 구입 → 소액결제 대금청구 (스마트폰 피해자)

그렇다면 어떻게 해야 스미싱 피해를 방지할 수 있을까요.

첫째, 각 통신사 고객센터에 전화하거나 통신사 인터넷 홈페이지를 이용하여 소액결제를 원천적으로 차단하거나 결제금액을 제한할 수 있습니다.

	통신사	고객센터를 통한 소액결제 차단방법
1	SKT	1) 자신의 스마트폰으로 114로 통화버튼을 눌러 SKT고객센터로 연결 → 2) ‘3’번을 눌러 상담원과 연결 → 3) 소액결제 모두 차단
2	KT	1) 100을 눌러 ‘5’번, 그리고 ‘1’번을 순차적으로 눌러 KT 모바일 고객센터로 연결 → 2) 상담원과 통화하여 오프라인결제 · 무선결제 · 청구대행 · 본인인증차단 등을 선택적으로 신청하여 소액결제 차단 ※ 자신의 스마트폰으로 114를 눌러 상담원과 연결해도 소액결제 차단 가능
3	LGU+	1) 자신의 스마트폰으로 114를 눌러 전화를 하면 LGU+고객센터로 연결 → 2) ‘0’번을 눌러 상담원과 연결 → 3) 자동결제 · 인증결제 모두 차단됨

둘째, 스마트폰용 백신프로그램을 설치하여 악성코드 설치를 차단합니다.

셋째, 확인되지 않은 앱(App)이 함부로 설치되지 않도록 내 스마트폰의
보안설정을 강화합니다.

※ 스마트폰의 보안설정 강화방법 : 환경설정 > 보안 > 디바이스 관리 >
‘알 수 없는 출처’에 V체크가 되어 있다면 해제

넷째, ‘쿠폰’, ‘상품권’, ‘무료’, ‘조회’, ‘공짜’ 등으로 스팸 문구를 미리
등록하여 내 스마트폰에 스팸 문자가 전송되는 것을 사전에
차단하는 방법이 있습니다.

※ 스마트폰내 스팸 문자발송 차단방법 : 문자메시지로 들어가서 ‘설정 >
스팸 메시지 설정 > 스팸 문구로 등록’을 클릭

다섯째, T스토어 · 올레마켓 · U+앱마켓 등 공인된 오픈마켓을 통해
앱(App)을 설치할 것을 권고합니다.

마지막으로, 유료게임을 공짜로 즐기기 위해 인터넷에서 apk파일을
다운받아 스마트폰에 저장하지 마십시오. apk파일의
특성상 악성코드 앱이 심어져 있을 가능성이 높습니다.

위와 같이 ‘스팸 피해 예방법 6가지 수칙’을 여러분께서 지켜주신다면,
우리의 소중한 정보와 재산은 범죄로부터 보호할 수 있습니다.

새해 복 많이 받으시고, 항상 행복하시길 기원합니다. 감사합니다.

경찰청 사이버테러대응센터