건강한 금융생활정보 가이드

2020-03호

01_당첨 됐다던 추석이벤트 알고 보니 스미싱 당첨?

07_우리를 속이는 메신저 피싱 사기범들의 말! 말! 말!

모두의 기쁨, 그 하나를 위하여
하나은행

자료출처: www.fss.or.kr

풍성하고 행복할 것만 같은 추석연휴를 앞두고 추석택배 배송 확인, 코로나19 관련 긴급재난 지원 및 결제 등을 사칭한 스미싱이 증가할 것으로 예상되어 각별한 주의가 요망되고 있습니다.

*스미싱 : 문자메시지(SMS)와 피싱(Phishing)의 합성어로 악성 앱 주소가 포함된 휴대폰 문자(SMS)를 대량 전송 후 이용자가 악성 앱을 설치하거나 전화를 하도록 유도하여 금융정보 · 개인정보 등을 탈취하는 수법(보이스피싱, 전자상거래 사기, 기타 다양한 사기에 광범위하게 이용)

실제로 올해 8월까지 스미싱 탐지 건수는 전년 동기간 대비 378% 증가
('19.1~8월 185,369건 → '20.1~8월 700,783건),

코로나19 관련 긴급재난지원금을 사칭한 스미싱이 등장('20.1~8월 10,753건)

행복한 추석명절 기간동안 성행할 수 있는 스미싱, 보이스피싱 피해를 예방하기 위해서 주요 스미싱 문자 예시와 스미싱 피해예방 수칙 및 피해발생 시 행동요령에 대해 알아보겠습니다!

최근 유행하고 있는

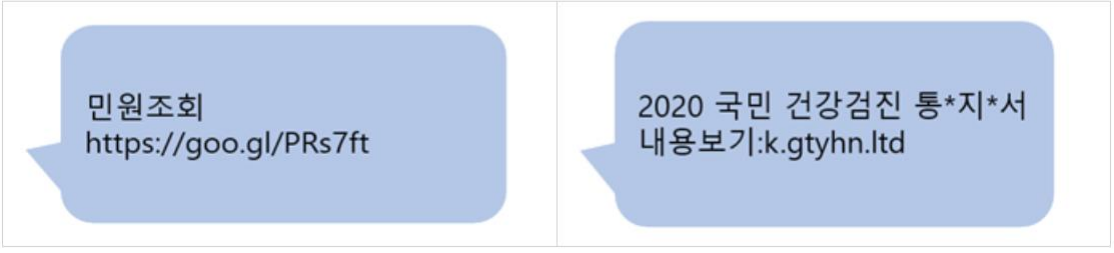
스미싱 문자 예시

택배 관련 스미싱,
공공기관 사칭 스미싱,
지인 사칭 · 선물 관련 스미싱,
코로나19 사칭 · 긴급재난지원금 관련 스미싱

아래 예시들을 참고하시고 이와 유사한 스미싱 문자가 온다면 고민하시지 마시고 삭제해주세요!

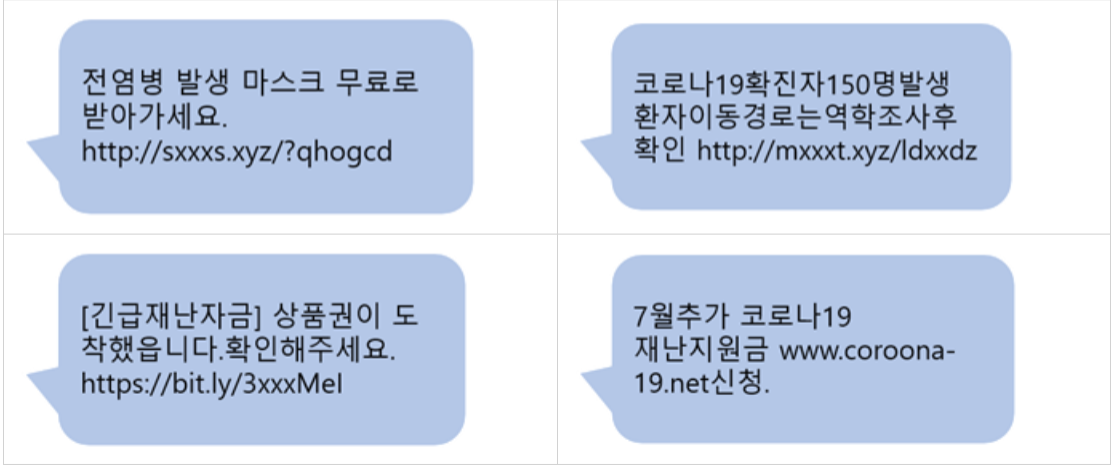
1. 택배 관련 스미싱

2. 공공기관 사칭 스미싱



3. 지인 사칭 · 선물 관련 스미싱

4. 코로나19 사칭 · 긴급재난지원금 관련 스미싱



이것만 기억해주세요

스미싱 피해예방 수칙

1. 출처가 미확인된 문자메세지의 링크주소 클릭을 주의하세요!

택배 조회, 명절 인사, 모바일 상품권·승차권·공연예매권 증정 등의 문자 속에 출처가 확인되지 않은 인터넷 주소(URL)는 절대 클릭하시면 안됩니다.
특히, 긴급재난지원금 안내 문자에는 인터넷주소(URL) 링크가 포함되지 않으므로 문자내용에 인터넷주소를 클릭하지 않고 즉시 삭제하시기 바랍니다.

2. 스마트폰 보안설정을 강화하세요!

알 수 없는 출처의 앱이 함부로 설치되지 않도록 스마트폰의 보안설정을 강화하고, 앱 다운로드 시 출처가 불분명한 인터넷 주소(URL)에서 다운로드 받지 않고 공인된 앱마켓을 통해 다운로드 및 앱을 설치하세요.

3. 백신프로그램을 설치하세요!

이통사, 보안업체 등에서 제공하는 **백신프로그램을 설치**하여 **업데이트 및 실시간 감시상태를 유지**해야 합니다.

4. 소액결제를 차단 · 제한하세요!

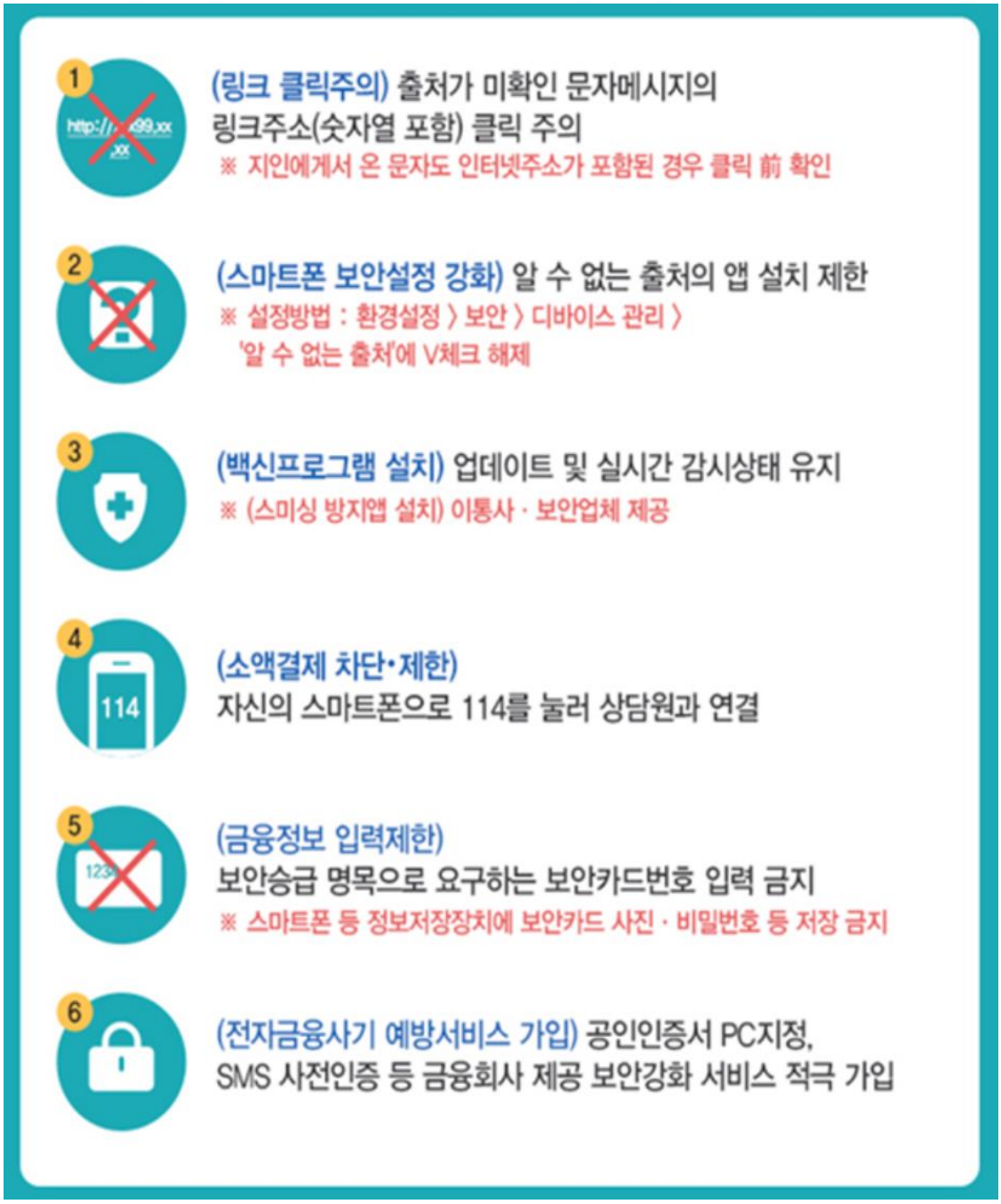
자신의 스마트폰으로 114에 전화해, 상담원과 연결을 해서 요청하실 수 있습니다.

5. 금융정보를 함부로 입력하지 마세요!

보안강화 및 업데이트 명목으로 **개인정보·금융정보를 요구**하는 경우 절대 **입력하거나 알려주시면 안됩니다.** 또한, 스마트폰 등 정보저장장치에 **보안카드 사진 및 비밀번호 등을 저장하시면 안됩니다.**

6. 전자금융사기 예방서비스에 가입하세요!

공인인증서 PC지정, SMS 사전인증 등 금융회사가 제공하는 **보안강화 서비스**에 적극적으로 가입함으로써 스미싱 피해를 예방하실 수 있습니다!



① **금융기관 콜센터 전화** : 경찰서에서 발급받은 '**사건사고 사실확인원**'을 이동통신사, 게임사, 결제대행사 등 관련 **사업자에 제출**합니다.

② **악성파일 삭제** : **스마트폰 내 '다운로드' 앱 실행** → 문자를 클릭한 시점 이후, 확장자명이 apk인 파일 저장여부 확인 → 해당 apk파일 **삭제**합니다.
※ 삭제되지 않는 경우, 휴대전화 서비스센터 방문 또는 스마트폰 초기화해야 합니다.

③ 한국인터넷진흥원 **118상담센터(국번없이 118) 상담**을 받습니다. 명절 연휴 중 **스미싱 의심 문자**를 **수신**하였거나 **악성앱 감염 등이 의심** 되는 경우 **국번없이** 118**상담센터로 문의**하시면 24**시간 무료로 상담** 받을 수 있습니다.

④ 금융 및 증권 등 **공인인증서 즉시 폐기 및 재발급**을 받습니다.

⑤ 이동통신사에 **모바일 결제내역** 여부를 **확인**합니다.

⑥ 사용 중인 **이동통신사**에서 제공하는 **스미싱 예방서비스(App 등)** 설치 및 활용합니다.

⑦ **주변 지인**들에게 스미싱 피해 사실을 즉시 알려 **2차 피해 발생 사전 방지**합니다.

⑧ 문자메시지 등으로 수신된 **금융회사 및 공공기관의 홈페이지**는 반드시 인터넷 검색 등을 통해 **정확한 주소**인지 **확인**합니다.

오늘은 언택트 사회에서 점점 진화해가고 있는 메신저피싱에 대해서 좀 더 알아보려고 합니다!

금융감독원에 따르면 언택트 사회로 전환이 가속화되면서 전형적인 언택트 범죄인 메신저피싱의 피해규모가 갈수록 증가하고 있다고 하는데요, 올해 1월~4월, 4개월간 그 피해액이 무려 128억원에 달한다고 합니다. 엄청난 금액이죠?!

일반적으로 메신저피싱은 카카오톡 등 SNS에서 가족이나 지인을 사칭해 피해자에게 돈을 요구하는 방법으로 이루어집니다. 금융감독원에서 메신저피싱 사기범들의 사기수법을 분석해본 결과 일반적인 패턴을 찾을 수 있었는데요, 사기범들은 과연 어떤 말을 하면서 우리를 속이려고 할까요?

1 "엄마.. 뭐해? 많이 바빠?"

사기범들은 "**엄마 뭐해?**", "**많이 바빠? 바쁜거 아니면 톡 해줘**"와 같이 가족이나 지인을 사칭하며 피해자 상태를 파악하기 위해 연락을 시도합니다.

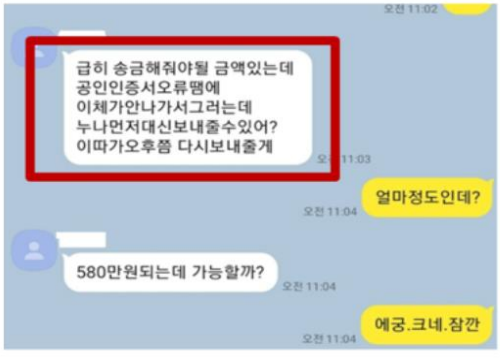
2 "핸드폰이 고장나서 컴퓨터로 하고있어.."

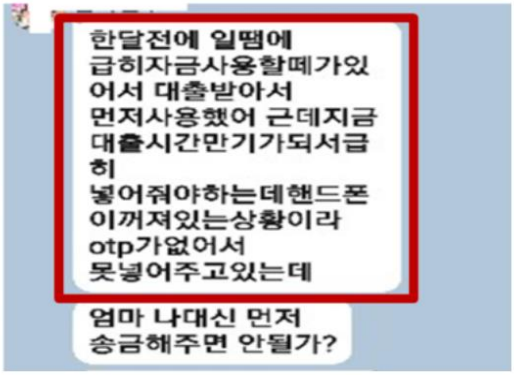
사기범은 가족이나 지인이 의심할 것에 대비해서 액정파손, 충전단자 파손, 공인인증서오류 등으로 휴대전화를 사용할 수 없어 PC카톡 등 컴퓨터를 이용해 연락하고 있다고 이야기합니다.

메신저피싱 사기범의 실제 대화내용

3 "지금 당장 돈이 좀 필요해..."

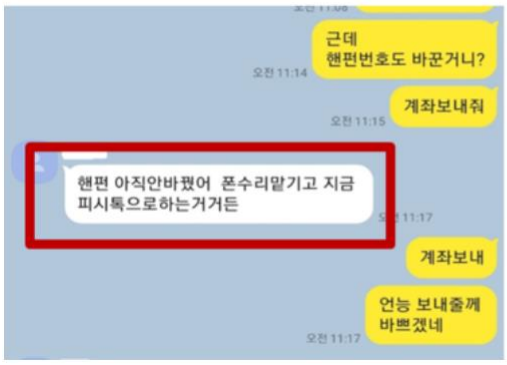
메신저피싱 사기범의 실제 대화내용

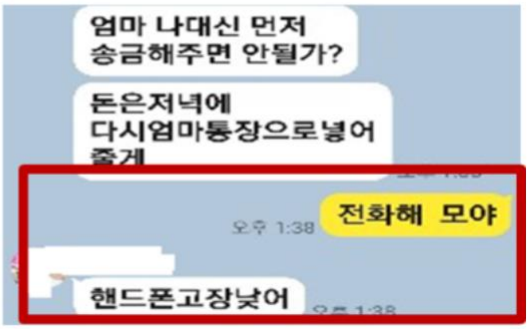




4 "핸드폰이 고장나서 지금은 통화 못해..."

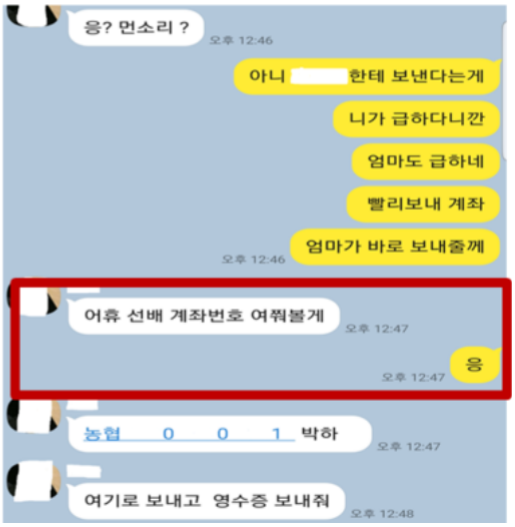
메신저피싱 사기범의 실제 대화내용





5 "내 계좌 말고 여기로 보내줘.."

메신저피싱 사기범의 실제 대화내용



6 "아직 안보냈어? 언제쯤 보낼거야?"

우리를 속이는 메신저피싱 사기범들의 말

▸ 문화상품권 구매 후 핀번호 전송 요구

- 계좌에 대한 지급정지를 피하기 위해 최근 주로 이용되는 수법으로, '문화상품권을 구매해야 하는데 카드 문제로 결제가 되지 않으니,
문화상품권 구매 후 핀번호를 보내주면 구매대금을 보내주겠다'고 속이는 방식

▸ 스마트폰에 '원격제어 어플'을 설치하도록 유도

- 스마트폰 사용이 익숙하지 않은 피해자에게 '팀뷰어' 등 원격제어 어플을 설치토록 유도한 후 해당 휴대폰을 직접 제어하거나 개인정보를 탈취해 온라인 결제 등을 통해 금전을 편취하는 방식

▸ 신용카드의 사진과 비밀번호 전송 요구

- 스마트폰 계좌이체나 온라인 상품권 구매 등에 익숙하지 않은 중장년층을 주된 타겟으로 삼는 수법으로, 카드 정보와 비밀번호를 요구한 후 이를 이용해 범인이 직접 상품권 등을 구매하는 방식

1 실제 가족, 지인이 맞는지 직접 전화통화로 확인

아무리 사기범이 휴대폰이 고장났다거나 휴대폰을 잃어버렸다고 이야기한다고해도, 돈을 송금하시기 전에는 반드시 직접 전화통화를 시도해보세요!

2 긴급한 상황이더라도, 전화 확인 전 송금 금지

앞서 말씀드렸듯이 사기범은 금융기관에서 대출을 받았는데 연체될까봐 걱정된다, 혹은 선배가 급하게 돈이 필요한상황이라고 이야기하는 등 긴급한 상황임을 강조하는 말들을 합니다.

가족이나 지인이 긴급한 상황을 앞세워 돈을 송금해줄 것을 독촉한다고 하더라도 언제나 전화 확인이 우선이라는 것 잊지 마세요!

3 타인계좌로 송금요청시 일단 의심

앞서 보여드린 예의 공통점은 바로 '타인계좌'로 송금요청을 해줄 것을 요청한다는 것입니다. 내 가족 또는 지인이 다른 사람의 계좌로 돈을 송금해줄 것을 요청할 경우, 일단 메신저피싱을 의심해보세요! 일단 의심부터 하게 되면, 메신저피싱에 당할 확률이 줄어듭니다!

※ 불가피하게 메신저피싱 피해가 발생한 경우,

은행(고객센터), 경찰(112 또는 182), 금융감독원(1332)에 즉시 신고하여 송금/이체한 계좌의 지급정지를 요청하세요!