ChatGPT

군 장병 맞춤형 피싱·스캠 예방 서비스 기획을 위한 심층 시장 조사 보고서

문제 정의: '일과 후 스마트폰'이 만든 새로운 공격면과 군 특수 리스크

핵심 요약
대한민국 군은 일과 후 병(兵) 스마트폰 사용이 제도화되며, 장병 개인의 금융·개인정보 위험이 '상시 노출' 형태로 바뀌었습니다.
이 노출은 단순한 개인 피해(계좌 탈취, 대출 유도)에 그치지 않고, 악성코드 감염·계정 탈취·연락처 확산을 통해 부대 보안사고(위치·시설·인원·업무 단서 노출)로 전이될 수 있다는 점에서 국가안보 리스크로 연결됩니다.

세부 데이터
방송·미디어 이용행태 조사 결과에서 스마트폰은 '필수 매체'로 급속히 자리 잡았고, 특히 10~30대에서 스마트폰을 필수 매체로 인식하는 비율이 90% 이상이라는 정부 발표가 있습니다.
같은 조사에서 전체 이용자 기준 일평균 스마트폰 이용시간이 2024년 2시간 6분으로 증가했다는 발표도 확인됩니다.
이러한 '상시 접속 환경' 위에서 문자·URL 기반 공격(스미싱)이 단기간에 폭증했고, 보이스피싱은 건당 피해액이 커지는 방향으로 재확대되는 추세가 정부·수사기관 자료에서 동시에 관측됩니다.

시각화 제안
'군 장병 스마트폰 허용(정책 변화) → 접속시간 증가(10~30대 필수매체) → 스미싱/보이스피싱 재확대 → (개인피해 + 부대보안 위험)'을 한 장의 **인과관계 흐름도(Problem Tree)**로 구성. 근거 수치로 10~30대 필수매체 인식(90%+)과 2024년 스마트폰 이용시간(2시간 6분)을 배치.

최근 트렌드: 스미싱 폭증과 보이스피싱 '고액화', 그리고 결합형 스캠의 출현

핵심 요약
최근 3개년(2023~2025) 한국의 피싱 위협은 "대량 유포(스미싱) + 고액 피해(보이스피싱) + 결합형 스캠(로맨스·투자·구제빙자 등)"으로 진화했습니다.
2026년을 전망하는 자료에서도 AI 기반 음성사기, 핀테크 악용 자금세탁, 해외 '스캠센터' 결합 등으로 범죄가 계속 진화할 것으로 제시됩니다.

세부 데이터
스미싱은 탐지·차단 지표에서 급증이 확인됩니다. 예를 들어 2024년 스미싱 탐지 건수가 200만 건대를 기록했고, 2023년 대비 크게 증가했으며 2025년에도 상반기부터 높은 탐지 규모가 이어졌다는 보도가 있습니다.
보이스피싱은 2025년 1~3월 발생 건수 5,878건, 총 피해액 3,116억 원으로 집계된 자료가 공개되어, 전년 동기(2024년 1~3월 5,015건·1,411억 원) 대비 피해 규모가 급증했음을 보여줍니다.
또한 2025년에는 "보이스피싱 피해액이 1조 원을 넘었고, 로맨스 스캠 등 신종 다중사기 피해액이 7천억 원 수준"이라는 보도도 있어 '다중 사기(Scam compound)'가 별도 축으로 커지고 있음을 시사합니다.

시각화 제안
① **이중축(line+bar) 차트**: (좌) 2023~2025 상반기 스미싱 탐지 규모, (우) 2024Q1 vs 2025Q1 보이스피싱 피해액 비교.
② **'위협 진화' 타임라인**: 2023(청년층 피해 증가 경향) → 2024(스미싱 대량 유포 재확대) → 2025(고액화·로맨스 스캠 성장) → 2026(AI 음성·스캠센터 결합 전망).

군 장병 특화 피싱 유형: ‘급여·휴가·군 신뢰(브랜드)’를 노리는 사회공학

핵심 요약
군 장병 표적 공격은 “군 조직 특유의 신뢰·위계·급여/휴가 체계”를 악용해 클릭·설치·정보입력을 유도하는 방식으로 구체화됩니다.
특히 군 명칭·직인·공문 등 ‘진짜 같은 증빙’이 동원되는 사례가 군 관련 사기에서 반복 관측되고 있어, 일반인 대상 피싱보다 ‘의심 임계치’를 낮추는 구조적 요인이 됩니다.

세부 데이터
군 급여·수당을 미끼로 한 스미싱이 실제로 보고되었습니다. 2024년 2월, 군 간부 등을 대상으로 군 재정 관련 기관을 사칭해 “명절휴가비 지급 안내”와 함께 ‘지급내역 확인’ 링크를 보내는 스미싱 문자가 유포되었고, 당국이 “링크 클릭 금지”를 공지한 사례가 보도되었습니다. (정상 급여 안내 채널과 ‘문자+링크’의 불일치가 핵심 경고 포인트로 제시됨)
군(軍) 신뢰를 악용한 사기는 “군 간부/부대 사칭 단체 주문 → 위조 공문·직인 전송 → 타업체 대금 대납 요구 → 연락두절” 유형으로 전국적으로 문제화되었고, 군 당국은 2024년 이후 누적 수백 건·수십억 원대 피해를 제시하며 ‘국방헬프콜 1303 등을 통한 신분 확인’을 강조했습니다.
군이 강제 설치를 요구하는 보안 앱·모바일 통제 체계 자체에서도 취약점 또는 운영 공백 문제가 지적되었고(예: 위치정보 등 민감정보 노출 가능성 주장, 플랫폼별 통제의 불균형 논란), 이는 “보안 앱/보안 점검/업데이트”를 사칭하는 피싱 메시지가 설득력을 얻기 쉬운 환경적 배경이 됩니다(※ 여기서 ‘피싱 메시지의 설득력 증가’는 취약점 논란이 **신뢰·혼란을 유발**한다는 점을 근거로 한 기획적 추론).

시각화 제안
① **군 특화 피싱 ‘3대 미끼’ 카드형 인포그래픽**: (1) 급여/수당/정산 (2) 부대/간부/공문 (3) 보안앱/보안점검. 각 카드에 실제 사례 1개씩(명절휴가비 스미싱, 군부대 사칭 노쇼, 보안앱 이슈)을 짧은 캡처/문구로 배치.
② **의사결정 포인트 강조 스토리보드**: “링크 클릭 전 3초(확인) → 클릭 후 3분(감염/탈취) → 부대 확산 3일(2차 피해)”의 시간축.

국가안보 리스크 시나리오: ‘개인 단말 감염’이 ‘부대 보안사고’로 확산되는 경로

핵심 요약
장병 스마트폰은 군 내부망과 물리·논리적으로 분리되어 있더라도, “개인 단말 안의 정보(연락처·메신저·사진·위치) + 외부 포털 계정 + 사회공학 확산”을 통해 보안사고의 기점이 될 수 있습니다.
또한 최근 국회 제출 자료 기반 보도에서 군을 대상으로 한 사이버공격 시도가 장기간에 걸쳐 높은 빈도로 발생(월평균 약 1,000건, 일평균 약 33건 수준)한 것으로 제시되어, ‘표적 환경’ 자체가 고위험임을 뒷받침합니다.

세부 데이터
군을 겨냥한 사이버공격 시도는 2020년부터 2024년 8월까지 총 5만6,034회로 제시되었고, 해킹메일을 통한 침해 시도가 전년 대비 급증했다는 분석도 함께 보도되었습니다.
군 보안 규정 위반은 최근 5년간 3,922명 수준으로 감사 결과가 보도되었으며, 비밀 취급·관리 소홀 등이 주요 위반 사례로 언급됩니다. 이는 “현장 보안 규정 준수의 변동성”이 크고, 개인 단말 기반 사고가 결합될 때 확산 통제가 어려울 수 있다는 현실 배경을 제공합니다.
공격 수법 측면에서, 문자/링크로 유도된 악성 앱이 원격제어 앱 형태로 설치되거나, 사용자가 ‘공식 스토어 화면’으로 착각하도록 위장해 설치를 유도하는 방식이 지속적으로 보고됩니다.

시나리오
시나리오 A: 급여 안내 스미싱 → 단말 감염 → 부대 단서 수집
장병이 “명절휴가비 지급” 링크를 클릭해 피싱 페이지에 접속하고, 그 과정에서 악성 앱/원격제어 앱이 설치됩니다(유사 수법은 실제 피해 사례와 보안 분석에서 반복 보고). 공격자는 단말 내 사진·연락처·메신저 알림 등을 통해 부대 인근 이동 동선·시설 단서를 수집하거나, 단체 채팅방에서 ‘훈련/근무 일정’ 단서를 확보해 2차 표적화를 수행합니다.

시나리오 B: 한 명의 감염 → ‘연락처 확산’으로 동기·간부까지 연쇄 타격
감염된 단말에서 연락처·메신저 기반으로 “지인/기관 사칭 링크”가 동시다발 발송되면, 같은 부대/동기 집단이 한 번에 공격을 받습니다. 표적형 피싱(스피어피싱)이 ‘맥락 특화 메시지’로 성공률을 높인다는 연구 흐름과, 시간 압박·권위(기관·상급자)를 결합한 메시지가 판단을 흐린다는 연구는 이 확산 메커니즘의 개연성을 보강합니다.

시나리오 C: ‘위치 노출’의 자동화 → 물리적 위협/심리전과 결합
군 관련 모바일 통제 앱에서 ‘부대/병사 위치 노출 가능성’이 지적된 바 있고, 병사들이 보안 앱을 임의로 삭제하거나 우회해 총기·장갑차 등 군 관련 이미지를 SNS에 게시한 사례도 보도된 바 있습니다. 이때 공격자는 OSINT(공개정보 수집)와 결합해 부대 위치·장비·부대 운영 단서를 체계적으로 수집해 심리전(허위정보·가짜 영상·협박) 또는 표적 공격(스피어피싱)으로 연결할 수 있습니다.

시각화 제안
‘개인 단말’에서 ‘부대 리스크’로 이어지는 **전파 네트워크 다이어그램**: (피싱 문자)→(클릭/설치)→(단말 권한)→(연락처/메신저 확산)→(부대 집단 감염)→(보안사고/심리전). 각 노드에 실제 근거 지표(군 사이버공격 일평균 33건, 보안 규정 위반 3,922명)를 숫자로 배치.

기존 해결책의 한계: 교육·보안앱·스팸차단이 ‘실시간 클릭 순간’을 못 막는 이유

핵심 요약
현재 대응은 대체로 (1) 사후 교육·캠페인, (2) 단말 통제 앱, (3) 통신/앱 기반 스팸차단에 집중되어 있습니다. 그러나 피싱의 승부처는 “링크 클릭 직전/직후 10초”이고, 이 순간에 **군 맥락을 이해한 실시간 판별**이 부재하면 피해가 발생합니다.
또한 장병 휴대폰에 대한 강제 점검은 인권·사생활 침해 논란이 지속될 수 있어 ‘검사·단속 기반’ 모델은 구조적 한계가 있습니다.

세부 데이터
보안 통제 앱은 우회·비활성화 논란이 반복적으로 제기되어 왔고, 플랫폼(예: iOS)에서의 통제 공백 문제가 지적된 사례도 보도되었습니다.
피싱이 URL(링크) 기반으로 확산되는 현실을 반영해, KISA가 ‘X-ray(엑스레이) 시스템’ 등으로 스미싱 사전차단을 추진하고, 일정 시점부터는 문자 내 URL 사전검증·차단 요구가 제도적으로 강화되는 흐름이 나타났습니다. 이는 “URL 중심 방어”가 정책적으로도 핵심 축이 됐음을 시사합니다.
피싱 메시지가 권위·긴급성(“기관입니다”, “지금 확인”)을 결합해 사용자의 비판적 판단을 약화시키는 메커니즘은 연구에서도 반복 확인되며, 특히 시간 압박은 사용자의 오류 가능성을 높이는 변수로 분석됩니다.

왜 ‘군 전용 실시간 URL 분석 서비스’가 필요한가
기술적 근거: 스미싱 URL은 대량 생성·단기 유통되며, 공격자는 탐지 회피를 위해 도메인·경로를 빠르게 바꿉니다. 탐지 건수 급증은 “정적 차단(블랙리스트)”만으로는 부족해졌음을 보여주는 간접 지표입니다.
심리적 근거: 장병 환경은 ‘시간 제약(점호·복귀·교육·외출 준비)’과 ‘권위/공식 채널처럼 보이는 메시지(급여·기관)’가 결합될 가능성이 높고, 이는 피싱 설득 기법(긴급성+권위)에 취약해지는 조건과 맞닿아 있습니다.
운영·정책적 근거: 사생활 침해 논란을 유발하는 단말 검사·열람 중심의 대응 대신, 사용자가 스스로 “클릭 전에 검증”할 수 있는 비침해적 도구가 필요합니다.

시각화 제안
Gap 매트릭스(표)를 슬라이드로 제시: 가로축 ‘공격 단계(유입→클릭→설치/탈취→확산)’ / 세로축 ‘현 대응(교육·보안앱·통신차단)’을 놓고, 공백이 가장 큰 칸을 ‘클릭 순간의 URL 판별’로 강조. 정책 트렌드(엑스레이 시스템/사전차단 강화)를 우측 상단에 ‘시장 요구의 제도적 신호’로 표시.

시장 및 사회적 가치: 전투력·사기·ESG 관점의 투자 논리

핵심 요약
군 장병 대상 피싱 예방은 '개인 금융보호 서비스'를 넘어, (1) 전투력 유지(심리 안정·집중력), (2) 부대 보안 리스크 감소(감염·확산), (3) 공공가치/ESG 실현(청년 보호, 범죄 예방)의 삼중 효과를 가질 수 있습니다.

세부 데이터
시장(수요) 규모의 최소 바닥은 '현역·상비 병력'입니다. 2025년 7월 기준 군 병력이 45만 명 수준으로 감소했다는 국회 제출자료 기반 보도가 있으며, 병력 감소 국면에서도 '개인 단말 기반 공격면'은 오히려 커질 수 있습니다(스마트폰 중심 생활의 고착).
사회적 비용 측면에서, 최근 2년 내 금융소비자의 절반가량이 금융사기에 "노출 또는 피해 경험"을 보고했고(조사 기반), 이는 장병도 같은 디지털 생태계에 있음을 보여주는 간접 지표입니다.
전투력·사기 논리의 근거로는, 미국 국방 정책·연구 문헌에서 "재정적 준비(financial readiness)가 군 가족/개인의 준비태세이며 궁극적으로 작전준비태세(operational readiness) 구성요소"로 명시된 바 있습니다. 또한 군 구성원의 재정적 어려움이 우울·불안 등 정신건강 지표와 연관된다는 연구도 보고됩니다(국가·제도 맥락은 다르나, '재정 충격→정신·업무 영향'의 일반 메커니즘 근거로 활용 가능).
사이버 측면에서도 "사이버 회복탄력성(cyber resiliency)은 준비태세(readiness)"라는 군 조직의 공식 메시지가 존재해, 장병 단말 보안이 넓은 의미의 준비태세와 접합될 수 있음을 보여줍니다.

시각화 제안
① **가치 피라미드**: (하단) 장병 개인 금융피해 감소 → (중단) 부대 보안사고 확산 억제 → (상단) 국가안보·준비태세 기여. 각 층에 근거 문구("financial readiness → operational readiness", "cyber resiliency is readiness")를 짧게 인용 요약.
② **ESG 매핑 슬라이드**: S(청년·장병 보호, 금융사기 노출 절반 수준의 사회문제 대응) / G(규정 준수, 사생활 침해 최소화 예방형 모델).

타겟 세대 분석: MZ/Alpha 장병의 미디어·보안 인식 특성과 공격 적합성

핵심 요약
현역 장병의 다수는 20대 초반 중심(디지털 네이티브)이며, 동시에 "스마트폰 필수 매체, 숏폼·OTT·메신저 중심" 이용 행태를 갖는 세대와 겹칩니다. 이들은 기술에 익숙하지만, '기관사칭+긴급성'에 의한 판단 왜곡과 '빠른 전파(단체 채팅·DM)' 구조 때문에 피싱의 매력적 표적이 될 수 있습니다.

세부 데이터
정부 조사에서 10~30대의 스마트폰 '필수 매체' 인식률이 90% 이상으로 제시되었고, 스마트폰을 통해 주 5일 이상 이용하는 주요 콘텐츠로 숏폼·OTT·실시간 스트리밍 등이 언급됩니다.
모바일 행동과 보안 인식의 '간극'도 확인됩니다. 개인정보보호위원회 조사에서 성인·청소년 모두 개인정보 보호의 중요성을 매우 높게 인식하지만, 동의 내용을 실제로 확인하는 비율은 성인 55%, 청소년 37%에 그쳤다는 발표가 있습니다("중요하다고 느끼지만 실제 행동은 생략" 패턴).
금융사기 측면에서, 최근 2년 내 금융사기 노출·피해 경험이 49.9%라는 조사 결과가 발표되어(온라인 설문 기반), 장병처럼 디지털 채널로 정보를 소비·거래하는 집단은 '노출 확률'이 구조적으로 높을 수 있음을 시사합니다.
또한 2023년 보이스피싱 피해 분석에서 "20대 이하 및 30대의 피해 증가"가 공식 자료 기반으로 요약되어, 사회초년생/청년층이 더 이상 안전지대가 아니라는 점을 보여줍니다.

시각화 제안
① **장병 페르소나 2종**(병/간부 또는 징집병/초임간부): '하루 루틴(업무 후 스마트폰) + 주요 앱(메신저·숏폼) + 위험접점(문자·DM 링크)'을 여정지도(Journey Map)로 표현. 인식-행동 간극(중요성 인식 vs 동의 확인) 수치를 '행동 저항' 포인트로 표기.
② **공격적합성(Attack Fit) 레이더 차트**: (시간 압박/권위 메시지/공식 채널 위장/집단 전파/링크 클릭 빈도) 5축. 연구 근거로 'time pressure'와 'authority/urgency' 축을 뒷받침.

용어 주석

핵심 요약
발표에서 혼선이 잦은 용어를 '짧고 재사용 가능한 정의'로 정리합니다. (필요 시 슬라이드 하단 각주로 그대로 사용 가능)

세부 데이터
스미싱: 문자메시지(SMS)와 피싱(phishing)의 합성어로, 문자 내 링크 클릭·앱 설치를 유도해 개인정보·금융정보 탈취 또는 소액결제를 유발하는 사기.
보이스피싱: 전화 음성 기반으로 기관·지인 등을 사칭해 이체·현금 전달·앱 설치 등을 유도하는 전화금융사기. (정부·수사기관 통계는 집계범위가 다를 수 있어 출처를 함께 표기하는 것이 안전)
큐싱(Qshing): QR코드에 악성 URL 또는 악성앱 설치 주소를 심어 유포하고, 이를 스캔한 사용자를 피싱/악성앱 설치로 유도하는 공격.
스미싱·큐싱 확인서비스: 카카오톡 채널 등에서 의심 문자/QR의 악성 여부를 판별·신고하도록 지원하는 대국민 서비스 (예: 118 상담, 통합신고대응센터 안내 포함).
스피어피싱: 특정 조직/개인 맥락에 맞춘 표적형 피싱으로, 일반 대량 피싱보다 '그럴듯함'이 높아 성공률이 커질 수 있다고 보고되는 공격 유형.

시각화 제안
'용어-한줄정의-예시' 3열 구성의 **슬라이드 하단 미니 글로서리 박스**(발표 전반에 반복 삽입). 스미싱/큐싱만 아이콘(문자/QR)으로 구분하면 비전공자 심사위원 이해도가 빠르게 상승.
