링크를 한데 모아 공유하는 서비스는 편리하다. 한 페이지에 내 블로그, 쇼핑몰, 예약 페이지, 소셜을 모두 엮어두면 방문자가 길을 잃지 않는다. 문제는 범죄자도 이 편리함을 안다는 점이다. 링크모음과 주소모음은 공격자가 트래픽을 가로채거나 결제 정보를 훔치기 위한 지름길이 되기 쉽다. 요즘 피싱 미끼로 흔히 쓰이는 문구를 떠올려보자. 무료넷플릭스 쿠폰, 한정 이벤트, 빠른 환급. 미끼가 달콤할수록 링크를 눌러보려는 유혹이 커지고, 한번 발을 들이면 계정과 카드가 함께 위험해진다.

여기서는 운영자와 사용자가 함께 적용할 수 있는 보안 강화법을 정리한다. 이중 인증을 현장에 맞게 설계하고, 피싱 동선을 끊어내는 실무 팁을 곁들였다. 무조건 최신 기술을 쓰자는 구호보다, 예산과 환경, 사용자 유형에 맞는 선택이 중요하다. 링크모음은 본질적으로 관문이기 때문에, 관문만 단단해도 피해를 크게 줄일 수 있다.

링크모음이 공격 표적이 되는 구조

링크를 모으면 트래픽이 집중된다. 공격자는 이 집중 지점을 바꾸거나 흉내 내는 방식으로 수익을 낸다. 방법은 거칠게 세 갈래다. 첫째, 진짜 링크 사이에 악성 링크를 끼워 넣는다. 둘째, 진짜 페이지와 똑같이 보이는 위장 링크모음을 따로 만든다. 셋째, 링크 클릭 시 중간에서 리디렉션을 돌려 광고 수익이나 악성앱 설치로 유도한다.

운영 경험상 광고 수익형 악성 리디렉션은 탐지가 어렵다. 운영자 본인에게는 정상 페이지를 보여주고, 특정 지역이나 기기에서만 리디렉션이 발동되도록 조건을 걸어두기 때문이다. 사용자가 모바일 사파리에서만 이상 행동을 보고한다면, 조건부 스크립트 삽입을 의심해야 한다. 또 하나 눈에 띄는 패턴은 인기 키워드로 유입을 낚는 방식이다. 무료넷플릭스, 무료 IPTV, 해외직구 초특가 같은 단어로 주소모음을 만들어 검색 상단을 노린 뒤, 외부 지갑 주소나 개인정보 입력을 유도한다. 링크모음이 공식 사이트처럼 보이기 때문에 초보 사용자는 URL 구조의 미세한 차이를 보지 못한다.

피싱의 해부학: 낚는 문구보다 낚이는 순간

피싱은 문구가 아니라 타이밍 싸움이다. 링크모음 페이지가 인증 또는 결제의 중간 단계처럼 보이게 연출되면, 사용자는 이미 마음의 비용을 지른 상태다. 버튼 하나만 더 누르면 혜택을 받거나 절차를 끝낼 수 있을 것처럼 느낀다. 여기서 공격자는 진짜와 거의 같은 입력 폼을 제시한다. 이메일과 비밀번호, 카드 앞 여섯 자리, 원타임 코드까지 순서대로 묻는다. 순서를 진짜 절차와 동일하게 맞추는 것이 핵심이다.

운영 중에 겪은 사례를 들면, 계정 연결을 돕는다고 소개된 링크모음이 있었다. 첫 화면은 유명 소셜의 아이콘과 약관 링크까지 자연스러웠다. 차이는 아주 작았다. 도메인이 .link로 끝났고, 연결하려는 서비스의 공식 도메인과 철자 한 글자가 달랐다. 사용자는 로그인 정보를 입력했고, 페이지는 곧바로 진짜 서비스로 리디렉션을 보냈다. 피해자

는 로그인에 성공했다고 생각했지만, 사실 백그라운드에서는 도난 계정으로 비밀번호 변경이 진행되고 있었다. 이 정도의 공들임이면 단순 경고 배너로는 막기 어렵다.

이중 인증의 현실적 옵션과 선택 기준

이중 인증은 비밀번호 탈취가 있어도 계정을 지키는 마지막 울타리다. 하지만 구현 방식이 제각각이라 잘못 고르면 불편만 커지고 보안은 빈틈이 생긴다. 현장에서 써본 방식들을 장단점과 함께 정리하면 다음과 같다.

TOTP 인증앱. 가장 널리 쓰이고 오프라인에서도 동작한다. 서버와 시드만 맞으면 30초 단위 코드를 생성한다. 백업이 관건이다. 기기 교체 때 시드를 옮기지 못하면 사용자가 갇힌다. 복구 절차와 백업 코드를 미리 제공해야 한다.

푸시 승인. 사용자가 휴대폰에서 승인 또는 거부를 누르는 방식이다. 편하지만 승인 피로가 생긴다. 꽤 많은 사용자가 의식 없이 승인 버튼을 누른다. 반드시 번호 일치, 위치 표시, 도전 통지 지연 방지를 기본 옵션으로 켜야 한다.

SMS. 접근성이 가장 좋다. 반면 SIM 스와핑과 가로채기 위험이 있다. 해외 로밍에서는 수신 지연이 잦다. 계정 복구용 보조 채널로만 두고, 기본 수단으로 쓰지 않게 유도하는 편이 안전하다.

하드웨어 키, FIDO2, 패스키. 피싱 저항성이 가장 높다. 브라우저와 도메인을 검증하기 때문에 가짜 페이지에서 코드를 요구해도 동작하지 않는다. 보급과 비용이 과제다. 팀 단위로는 관리자에게부터 단계적으로 배포하는 모델이 유효했다. 소비자 서비스라면 패스키를 옵션으로 열고, 전환율 데이터를 보며 확장하는 방식을 권한다.

백업 코드. 적어도 8개 정도의 일회용 코드를 발급하고, 초기 설정 때 파일로 저장하게 유도한다. 운영하다 보면 백업 코드를 사진으로 찍어 클라우드에 올리는 사용자가 많다. 보안 교육에서 이 부분을 따로 강조해야 한다.

여기서 중요한 판단 기준은 사용자 분포와 실패 비용이다. 로그인 실패가 매출 손실로 바로 이어지는 커머스 서비스는 푸시 승인과 패스키를 조합해 마찰을 줄이고, 커뮤니티나 지식 서비스처럼 계정 가로채기가 악용되기 쉬운 곳은 TOTP 이상을 기본값으로 권장하는 식이다.

이중 인증 구현 체크리스트

- 패스키 또는 FIDO2를 우선 지원하고, TOTP와 SMS는 보조 채널로 제공한다
- 백업 코드 발급과 안전한 저장 안내를 초기 온보딩에 포함한다
- 승인 알림에는 숫자 일치, 대략적 위치, 로그인 브라우저를 함께 표기한다
- 새로운 기기 등록 시 추가 검증 단계와 24시간 제한을 둔다
- 관리자, 결제 권한 계정에는 하드웨어 키 사용을 의무화한다

링크모음 운영 환경에서의 보안 설계

링크가 많아질수록 점검 포인트가 기하급수적으로 늘어난다. 운영자는 도구로 이 문제를 줄여야 한다. 먼저 링크 저장 시 URL 정규화와 차단 목록 대조가 기본이다. 국제화 도메인에서 혼동을 일으키는 유사 문자, 가령 라틴 a와 키릴 a의 혼용을 탐지하는 규칙이 필요하다. 짧은 링크는 자체 단축 도메인을 운영해 리디렉션 경로를 통제하고, 외부 단축 링크는 펼쳐보기로 실주소를 노출하자.

클라이언트 측 방어도 중요하다. 링크를 새 탭으로 열 때는 rel 속성에 noopener와 noreferrer를 붙여 탭 간 침투를 막는다. 자바스크립트 위젯을 외부에서 끌어오는 경우에는 서브리소스 무결성 해시를 붙여 변조를 탐지한다. 콘텐츠 보안 정책으로 외부 스크립트, 프레임, 이미지 도메인을 흰색 목록으로 묶어두면, 공격자가 임의 스크립트를 삽입해도 실행되지 않는다. TLS는 HSTS까지 설정하고, 쿠키는 Secure와 HttpOnly, SameSite 옵션을 기본으로 한다.

분석 도구를 과하게 믿지는 말자. 자동 탐지의 임계값은 높여야 하고, 결정적 탐지는 사람이 해야 한다. 직접 운영하면서 효과를 본 접근은 세 가지다. 링크 클릭 후 평균 체류 시간이 비정상적으로 짧고 이탈률이 갑자기 오르는 링크를 우선 점검 목록에 올린다. 공통 UTM 태그를 가진 링크에서 환불 요청이나 계정 탈취 보고가 늘면 캠페인 단위

로 선 차단한다. 사용자 신고 폼에서는 링크 선택 입력을 자동 완성으로 제공해, 신고 데이터의 속도와 정밀도를 모두 챙긴다.

피싱 방지 체크리스트

- 링크에 유입되는 문구에서 무료, 한정, 인증 보너스 같은 강한 미끼 단어가 반복되면 우선 경고 배지를 띄운다
- 외부로 나가는 결제, 로그인, 배송조회 링크에는 도메인 미리보기와 인증서 발급자 정보를 함께 노출한다
- QR 코드로 전달되는 링크는 카메라 내부 브라우저가 아닌 기본 브라우저로 열리게 강제한다
- 주소모음에 사용자 생성 링크를 허용한다면 첫 7일은 클릭 수 제한과 추가 리뷰를 적용한다
- 피싱 신고가 접수되면 즉시 링크 단절, 연쇄 링크 추적, 유사 도메인 선제 차단을 순서대로 처리한다

사용자 교육은 문장 하나로도 바뀐다

온보딩에서 긴 경고문을 붙여도 거의 읽히지 않는다. 대신 행동 직전에 한 문장을 보여주는 편이 효과적이다. 예를 들어 결제 링크를 누르기 직전, 도메인 끝 부분이 기업 공식 도메인과 일치하는지 체크하자는 문장을 작게 배치하는 식이다. 이메일 인증 코드 입력 창에는 코드 공유를 요청하는 알림은 모두 사기라는 문구를 함께 보여준다. 웃긴 이야기 같지만, 이 한 줄이 팀 내부 테스트에서 오입력률을 20퍼센트 가까이 줄였다.

아이콘과 색도 중요하다. 경고 배지를 지나치게 자주 쓰면 경고 무감각이 생긴다. 사용자 리서치에서 배운 팁은 녹색 성공 배지와 빨간 경고 배지를 같은 무게로 쓰지 말라는 것이다. 경고는 더 적고 무겁게, 성공은 더 자주 가볍게. 링크모음의 경우 타사 로그인 버튼은 공식 아이콘 가이드라인을 지키고, 자체 제작 버튼은 색을 과용하지 않는다.

링크 짧게, 도메인은 길게

링크 단축은 편의와 추적을 동시에 준다. 그러나 외부 단축 도메인은 신뢰를 빠르게 떨어뜨린다. 사용자 조사에서 가장 불안해하는 요소가 무엇인지 물으면, 예측 불가능한 리디렉션이 첫손에 꼽힌다. 링크모음을 운영한다면 자체 도메인으로 짧은 링크를 만들자. 예를 들어 example.com/a, example.com/promo 같이 미리 보기로도 목적지를 가늠할 수 있게 구성한다. 이렇게만 해도 무료넷플릭스 쿠폰 같은 문구가 들어온다 해도, 최소한 도메인 신뢰에서 첫 관문을 통과해야 한다.

도메인은 누구나 볼 수 있는 신뢰의 기초다. 공식 사이트는 DNSSEC을 적용하고, 인증서는 조직 검증을 진행한다. 모바일에서는 인증서 정보 접근이 어렵긴 하지만, 운영자는 인증서 발급자와 만료일을 페이지 하단에 간단히 표기할 수 있다. 일부 고객은 이 한 줄에서 안심한다.

악성 확장 프로그램과 브라우저 보안의 맹점

많은 사용자가 링크를 클릭하는 환경은 브라우저다. 브라우저 확장 프로그램이 과도한 권한을 갖고 있으면 링크 안전성은 무의미해진다. 현장 이슈 중 하나는 방문 페이지에 스크립트를 삽입해 로그인 입력을 복사하는 확장 프로그램이었다. 크롬 웹 스토어에서 내려갔지만, 사용자 기기에는 계속 남아 있었다. 운영자 관점에서 할 수 있는 일은 제한적이지만, 로그인 페이지에서 붙여넣기 이벤트를 감시하고 비정상 입력 패턴을 식별하는 정도의 방어는 할 수 있다. 연속된 같은 문자, 마우스 이동 없이 초단위 내 완성되는 필드 입력 같은 신호를 기준으로 추가 검증을 요구하면 피싱 자동화의 성과를 낮출 수 있다.

모더레이션의 속도와 정확도 사이

사용자 제출 링크를 받는 구조라면 모더레이터가 생명줄이다. 자동 필터가 주소모음 80퍼센트를 거른다고 해도, 나머지 20퍼센트가 문제를 만든다. 실제로는 속도를 기준으로 등급을 나눠 처리하는 것이 현실적이다. 신고가 들어오면 우선 노출을 일시 중단하고, 동일 도메인의 다른 링크 노출도 잠시 멈춘다. 이후 사람이 개별 링크를 검토한

다. 승인된 링크에는 신뢰 점수를 부여해 재검토 주기를 늘린다. 표면적으로는 단순해 보이지만, 이 점수제 덕분에 팀의 주간 검토량을 절반 가까이 줄일 수 있었다.

사용자에게도 책임을 나눠 갖게 하자. 링크 상세에 "이 링크는 사용자 제출입니다" 같은 간단한 라벨을 붙이고, 제출자의 프로필 평판을 노출한다. 프로필이 빈약하고 제출 이력이 과하게 많은 계정은 별도 표시한다. 익명 제출을 허용해야 한다면 클릭 수와 지역 조건에 제한을 둔다.

사고 대응은 24시간 안에 매듭짓는다

모든 예방이 실패하는 날도 온다. 그날의 손해를 줄이는 비법은 시간 관리다. 내부 가이드에서는 24시간을 세 단계로 나눈다. 0시간에서 4시간 사이에는 링크 차단과 통지, 추가 피해 확산 차단이 전부다. 4시간에서 12시간 사이에는 피해 범위 추정과 결제사, 소셜 플랫폼 신고를 마친다. 12시간에서 24시간 사이에는 사용자 통지와 추가 교육, 복구 절차 안내를 일괄 배포한다. 실제로 이 리듬을 지키면 커뮤니티에서의 신뢰 손상을 최소화할 수 있다.

한 번은 해외 SMS 수신 지연으로 이중 인증 코드가 늦게 도착했고, 사용자는 조급함에 검색으로 문제 해결을 시도했다. 검색 상단에 있던 링크모음이 가짜 고객센터로 연결했고, 결국 기프트카드 충전 피해가 났다. 이 케이스에서 배운 점은 정식 고객센터 링크를 링크모음 상단 고정으로 배치하고, 해외에서 인증 코드가 지연될 때의 대체 경로를 눈에 띄게 안내해야 한다는 것이다.

엣지 케이스를 미리 걷어내는 설계

공용 PC와 공유 기기. 피시방이나 카페에서 로그인하는 사용자는 자동 저장과 세션 유지가 예상보다 큰 위험 요인이 된다. 공용 환경에서 로그인할 때는 자동으로 짧은 세션을 부여하고, 브라우저 창 닫힘 감지를 통해 세션을 제거하는 간단한 스크립트가 도움이 된다. 링크모음에서 외부 결제로 나가는 경우에는 세션이 유지되는지 여부를 교차 점검한다.

피처폰 또는 구형 스마트폰. TOTP 앱 설치가 어려운 환경에서는 음성 통화 인증이 의외로 유용하다. 로밍 환경에서도 음성은 문자보다 안정적이다. 단, 수신 가능한 시간대를 사용자가 지정할 수 있게 만들면 실패율이 크게 줄어든다.

해외 수신 지연. 해외 사용자 비율이 일정 수준을 넘으면, SMS를 기본 옵션에서 내려야 한다. 메시징 게이트웨이를 두 곳 이상 두고 자동 페일오버를 구성하면 체감 문제를 줄일 수 있다.

시각 장애 사용자. 화면 낭독기에서 이중 인증 흐름이 끊기지 않도록 라벨을 치밀하게 붙여야 한다. 6자리 코드 입력을 한 칸씩 나누어 디자인하면 접근성이 크게 떨어진다. 하나의 입력 필드로 통합하고, 자동 포커스 이동을 꺼야 한다.

지표로 확인하는 보안의 체감 효과

보안은 체감이 어려워서 지표가 필요하다. 로그인 성공률은 해석에 주의해야 한다. 이중 인증을 도입하면 단기적으로 하락한다. 대신 재인증 성공률, 기기 등록 소요 시간 중앙값, 이의 제기 건수 대비 승소율 같은 지표를 함께 본다. 피싱과 연동해서는 신고 건수와 허위 신고 비율, 차단된 링크의 재등재 비율, 클릭 대비 이탈률의 급상승 감지 건수를 주 지표로 사용한다.

A/B 테스트는 보안에서도 유용하다. 도메인 미리보기 배지의 문구를 바꾸거나 위치를 조정하는 것만으로도 링크 클릭 후 평균 체류 시간이 달라진다. 실험에서 가장 효과가 큰 변화는 배지의 위치였다. 링크 오른쪽 끝보다 제목 바로 아래에 배치를 바꿨을 때, 가짜 도메인에서의 즉시 이탈이 30퍼센트 가까이 늘었다.

법적, 윤리적 고려

링크 차단은 표현의 자유와 충돌할 때가 있다. 근거를 준비해두자. 서비스 약관에는 악성코드, 피싱, 무단 결제 유도, 개인정보 과도 수집을 금지한다는 조항이 명확해야 하고, 차단 사유를 사용자에게 통지하는 절차가 있어야 한다. 과도 수집의 기준은 법령과 가이드에 맞춘다. 주민등록번호, 운전면허번호, 은행 계좌 전체 번호는 비상 상황이 아니라면 필요하지 않다. 수집 목적을 적지 않은 링크에는 경고 배지를 자동으로 붙이고, 일정 기간 내 수정 요청에 응하지 않으면 비노출한다.

개인정보 보호 관점에서는 이중 인증 데이터의 저장과 복구가 민감하다. TOTP 시드는 암호화 저장하고, 복구 과정에서는 고객센터 직원이 사용자 계정에 직접 접근하지 못하게 권한을 쪼갠다. 내부에서 본 가장 흔한 실수는 복구 요청이 오면 직원이 임의로 이중 인증을 꺼주는 것이다. 이 절차는 반드시 이중 승인과 로그 감사를 통과해야 한다.

운영자와 사용자가 함께 지키는 습관

링크모음의 신뢰는 한 번의 사고로 무너질 수 있다. 운영자는 기술적 방어와 절차적 통제를 갖춰야 하고, 사용자는 작은 의심의 습관을 가져야 한다. 무료넷플릭스 같은 문구를 보는 순간, 도메인을 먼저 본다. 비밀번호를 입력하기 전, 브라우저 주소창의 자물쇠와 도메인 철자를 확인한다. 이중 인증을 설정할 때, 백업 코드를 안전한 곳에 보관한다. 이 간단한 습관이 실제 피해를 절반 이상 줄인다.

마지막으로 강조하고 싶은 점이 하나 있다. 보안은 완성품이 아니다. 링크 생태계와 공격 도구는 매달 바뀐다. 새로운 링크 유형이 등장하면 위협 모델을 다시 그려야 한다. 서비스가 성장할수록 공격자는 더 정교해지고, 운영자는 더 단순하고 강한 규칙을 원한다. 이 두 힘의 균형을 잡는 유일한 방법은 측정과 피드백이다. 데이터를 보고, 사용자를 듣고, 작은 실험을 계속 돌리자. 그러면 링크모음은 편리함과 안전을 함께 가질 수 있다.