Microsoft

# 멀티팩터 인증은 사이버 공격을 억제하는 데 얼마나 효과적일까요?

**루카스 아우구스토 마이어**
착한 실험실을 위한 AI

**톰 버트**
고객 보안 및 신뢰

**세르지오 로메로**
신원 보안

**알렉스 와이너트**
신원 보안

**가브리엘 베르톨리**
신원 보안

**후안 라비스타 페레스**
착한 실험실을 위한 AI

이 연구에서는 인증정보 유출이 확인된 계정을 중심으로 무단 액세스로부터 상업용 계정을 보호하는 데 있어 다단계 인증(MFA)의 효과를 조사합니다. 저희는 수동 계정 검토와 함께 벤치마크-승수 방법을 사용하여 의심스러운 활동을 보이는 Microsoft Azure Active Directory 사용자의 대규모 데이터 세트에서 다양한 MFA 방법의 보안 성능을 평가합니다. 조사 결과, MFA를 구현한 계정의 99.99% 이상이 조사 기간 동안 보안을 유지하면서 뛰어난 보호 기능을 제공하는 것으로 나타났습니다. 또한, MFA는 전체적으로는 99.22%, 자격

증명이 유출된 경우에는 98.56%까지 침해 위험을 줄였습니다. 또한 Microsoft Authenticator와 같은 전용 MFA 애플리케이션이 SMS 기반 인증보다 성능이 뛰어나지만, 두 방법 모두 MFA를 사용하지 않을 때보다 훨씬 강화된 보안을 제공한다는 사실도 입증했습니다. 이러한 결과를 바탕으로 보안을 강화하고 무단 액세스 위험을 완화하기 위해 상업용 계정에서 MFA를 기본적으로 구현할 것을 강력히 지지합니다.

Microsoft

# 소개

지난 10년 동안 Microsoft, Google, Okta와 같은 저명한 ID 공급업체들은 무단 액세스에 대한 보안을 강화하기 위해 *챌린지라고도 하는* 위험 기반 인증을 점점 더 많이 채택하고 있습니다. 이러한 챌린지는 IP 지리적 위치, 디바이스 및 IP 주소 평판, 로그인 시도 간격 등 다양한 수동적 신호를 활용하여 비정상적인 로그인 시도를 식별합니다. 불규칙한 로그인 패턴을 감지하거나 사용자의 비밀번호 변경 요청을 받으면 ID 공급자는 보호된 리소스에 대한 액세스 권한을 부여하기 위해 추가 인증 양식을 요청하는 챌린지를 발행합니다[1].

추가 인증 방법은 지식(사용자가 **알고** 있는 것), 소유(사용자가 **가진 것)**, 내재(사용자가 가진 것)의 세 가지 *요소로* 분류할 수 있습니다. 인증 체계에 보조 인증 요소가 필요한 경우 이를 2단계 인증(2FA)이라고 합니다. 좀 더 광범위하게, 다단계 인증(MFA)은 사용자가 인증 메커니즘에 두 가지 이상의 요소를 제시해야 하는 인증 방법을 포괄합니다[2].

소비자 계정을 인증하는 데 필요한 요소는 매우 다양하지만, 기업에 인증 서비스를 제공하는 Microsoft, Okta와 같은 회사는 주로 사용자가 소유하고 있는 디바이스로 코드를 전송하는 소유 확인 방식을 요구합니다[3]. 코드 생성 및 전송 방법에는 SMS, Microsoft Authenticator와 같은 전용 모바일 애플리케이션 또는 Yubikey와 같은 인증 전용 디바이스[4] 등 다양한 방법이 존재합니다. 이러한 추가 인증 수단을 사용하려면 사용자는 자신의 계정에 해당 수단을 사전 등록해야 합니다. 그러나 보조 디바이스에서 코드를 사전 등록하고 자주 확인해야 하는 번거로움이 증가하면 잠재적으로 채택률이 감소하고 계정 잠금이 증가할 수 있습니다[5, 6].

# 이전 연구와 우리의 기여

이전 연구에서는 Microsoft 계정(MSA) 및 Google 계정과 같은 소비자 계정에 대한 다단계 인증(MFA) 챌린지의 효과를 조사한 결과, 1) MFA 챌린지가 계정 유출을 방지하는 데 매우 효과적이며, 2) 일부 유형의 추가 인증 양식은 다른 유형보다 계정 유출을 방지하는 데 더 효과적이며, 3) 예방 효과, 도입 용이성 및 사용 편의성 간에 상충 관계가 있다는 사실을 발견했습니다[5, 7, 8, 9]. 최근에는 MFA의 지속적인 효과에 대한 의문이 제기되고 있습니다[10, 11].

소비자 계정은 널리 퍼져 있으며 주로 개인 이메일, 미디어 개인화, 인스턴트 메시징 등 무료 서비스에

대한 액세스 권한을 부여합니다.

메시징. 반면, 기업 및 정부 기관에서 직원과 고객에게 제공하는 계정은 결제 정보, 집계된 재무 데이터가 포함된 서버, 전산 리소스 등 다양한 유형의 데이터와 리소스에 대한 액세스 권한을 부여하는 경우가 많습니다. 이러한 상업용 계정은 Microsoft의 Azure Active Directory(AAD) 및 Okta의 Workforce Identity Cloud와 같은 상용 ID 제품의 보호에 의존하는 경우가 많지만, Amazon과 같은 일부 대형 공급업체는 자체 사내 솔루션을 사용하기도 합니다[3].

측정 기간 동안 상업용 계정은 특정 달에 사용된 전체 계정의 약 1/3을 차지했습니다. 소비자 계정 사용자와는 다릅니다,

인증 공급업체에 직접 등록하는 것과 달리, 상업용 계정 사용자는 테넌트 관리자라고 하는 중간 계층(일반적으로 소속 기관)에 등록해야 합니다. 예를 들어, 대학교 교수의 계정은 Microsoft와 같은 ID 공급자가 최종적으로 인증 서비스를 수행하더라도 대학교 자체에서 제공합니다. 이 예에서 테넌트 관리자인 대학은 계정을 등록 및 유지하고, 어떤 리소스에 MFA가 필요한지, 사용할 MFA 유형은 무엇인지 등 보안 정책을 정의하고, 일차적인 지원을 제공할 책임이 있습니다[12].

소비자 계정 데이터도 때때로 가치가 있을 수 있지만, 일반적으로 상업용 계정에 대한 접근 권한을 얻는 것이 더 가치가 있습니다[13]. 따라서 악의적인 공격자는 상업용 계정을 목표로 더 많은 시간과 리소스를 투입할 수 있으며, 이로 인해 상업용 계정에 대한 MFA의 효과가 달라질 수 있습니다. 이 백서에서는 상업용 계정에 적용된 보안 솔루션의 효과를 평가하고 이러한 결과를 소비자 계정에 대해 수행된 이전 연구와 비교하는 데 중점을 둡니다.

## 방법론 및 데이터

저희의 목표는 상업용 계정 모집단에서 계정 유출을 방지하는 데 있어 MFA의 효과를 확인하는 것입니다. 일반적으로 인증 제공업체는 샘플링 및 수동 검토에 의존하지 않고는 전체 모집단에서 계정 유출 건수를 정확히 파악할 수 없습니다. 사용자가 계정 유출을 감지하면 단순히 비밀번호를 변경하고 관리자에게 알리지 않을 수 있습니다. 관리자에게 알림을 받더라도 인증 제공업체에 알리지 않을 수도 있습니다. 따라서 신고된 계정 유출을 인증 제공업체에 의존하는 방식은 실제보다 과소 계상되는 결과를 초래합니다. 반면, 수십억 개의 계정을 보유한 인증 제공업체가 의심되는 모든 침해 사고를 수동으로 검토하는 것은 비용이 많이 듭니다. 따라서 샘플링 방법에 의존할 수밖에 없습니다.

저희는 목표를 달성하기 위해 2022년 4월 22일부터 2022년 9월 22일 사이에 의심스러운 활동으로 인해 계정이 검토된 활성 Microsoft Azure Active Directory 사용자 목록을 확보했습니다. 일부 계정은 MFA가 구성되어 있었고 일부는 그렇지 않았습니다. 계정이

에 의심스러운 활동이 있고 MFA가 설정되어 있으면 자동으로 챌린지가 발령되었습니다. 계정 로그를 검토하는 전문 팀이 세션 샘플을 소급하여 검토하고 침해 발생 여부를 결정합니다. 침해가 감지되면 해당 계정이 삭제되고 사용자에게 알림이 전송됩니다.

전체 인구에서 유출된 계정의 비율을 추정하기 위해, 개인이 실제 사건의 빈도를 과소 보고하는 경향이 있는 상황에서 역학 연구에서 일반적으로 사용되는 벤치마크 승수 방법[14]을 사용합니다. 벤치마크 승수법에는 두 개의 데이터 세트가 필요합니다. 하나는 벤치마크이며, 인구의 하위 그룹에 대해 연구 중인 이벤트의 완전하고 정확한 카운트를 가지고 있습니다. 다른 데이터 세트는 모집단의 대표 표본으로, 벤치마크가 나타내는 모집단의 비율을 추정하는 데 사용됩니다. 이 비율의 역수를 승수라고 합니다.

저희의 경우 벤치마크는 계정 전문가가 수동으로 검토한 계정 집합입니다.  이 데이터 세트의 경우

유출된 계정의 정확한 수를 파악하고 있습니다. 벤치마크는 두 가지 MFA 카테고리(MFA 사용 및 MFA 미사용)로 나뉩니다. 벤치마크를 전체 모집단과 연결하기 위해 각 카테고리별로 전체 모집단에서 무작위로 샘플을 추출하여 벤치마크에 포함된 계정 중 유출된 계정의 비율 π를 계산합니다.

15]에 제시된 방법론을 사용하여 다음과 같은 경우
크기 $N$의 벤치마크 $_x$ 및 확률 π
를 벤치마크에 포 함 할 대표 표본의 구성원에 대해, 모집단에서 손상된 계정 수인 $N_y$ 을 다음과 같이 추정할 수 있습니다.

$$\hat{N}_y = \frac{\hat{N}_x}{\hat{\pi}}$$

각 카테고리에 대해 [16]에 따라 비율 π는 π~ β($x$ + 1, $n$ + $x$ + 1) 분포하며, 여기서 $n$은 대표 표본의 크기이고 $x$는 벤치마크의 특성을 공유하는 해당 표본의 구성원 수입니다. 또한, $N_x$ 과 π 가 비편향적이더라도 π 에 대한 비선형성으로 인해 $N_y$ 은 $N_y$ 의 편향된 추정치이므로 [16]에 따라 편향 보정 추정치를 사용합니다:

$$\hat{N}_y = \frac{\hat{N}1_x}{\hat{\pi}} - \frac{(1-\hat{\pi})}{n} N_x \frac{}{\hat{\pi}}$$

몬테카를로 시뮬레이션을 사용하여 각 카테고리에 대해 $N_y$ 을 추정합니다. 각 시뮬레이션을 1,000회 실행합니다. 95% 신뢰 구간은 1,000회의 시뮬레이션 추정치의 2.5% 및 97.5% 백분위수를 기준으로 합니다. 비율 π에 대한 추정치는 표 1에 나와 있습니다.

## 결과

| 카테고리 | $\hat{\pi}$ (95% CI) | (a) | (b) | (c) |
|---|---|---|---|---|
| MFA 사용 | 2.20% - 3.01% | 1,525 | 59,414 | 0.0079% |
| MFA 없음 | 0.18% - 0.26% | 15,195 | 7,085,925 | 1.0071% |

*표 1: MFA 사용 및 미사용 결과*

결과는 표 1에 나와 있으며, (a)는 벤치마크에서 측정된 침해 건수, (b)는 모집단에서 추정된 침해 건수의 중앙값, (c)는 모집단에서 추정된 침해 건수의 중앙값 백분율입니다.

이러한 추정치에 따르면 MFA 계정의 예상 침해율 중간값은 다음과 같습니다.
는 0.0079%이며, 이는 MFA 계정의
99.99% 이상의 보호 계수

또한 백신 효과를 계산하는 데 사용된 것과 동일한 공식을 사용하여 위험 감소 비율로 효과를 계산합니다. MFA로 치료받은 인구의 위험 중앙값은 0.0079%로 추정되는 반면, MFA로 치료받지 않은 인구의 위험 중앙값은 1.0071%로 추정됩니다.

따라서 MFA 사용의 위험 감소는 다음과 같습니다.

$$\pi = 1 - \frac{\text{치료}}{} = 1 - \frac{0.0079\%}{} = 99.22\%$$

Microsoft

1.0071%

를 상업용 계정의 경우 이전에 소비자 계정에 대한 추정치와 일치하는 것으로 나타났습니다.

치료 없음

MFA의 효과를 측정하는 또 다른 방법은 2020 RSA 컨퍼런스[17]에서 Microsoft가 공유한 것처럼 MFA를 사용하도록 설정한 계정과 사용하지 않은 계정에서 발생하는 계정 침해 비율을 계산하는 것입니다.

데이터에서 침해의 중간 추정치를 사용하면 1 - $\frac{59,414}{(7,085,925+59,414)}$ = 침해의 99.17%라는 것을 알 수 있습니다.

계정에 MFA가 활성화되지 않았습니다. 이는 2019년 [17]에서 조사한 수치보다 약간 낮은 수치입니다. 하지만 2019년과 2022년 사이에 MFA 도입이 400% 이상 증가한 것으로 나타났습니다.

## 유출된 것으로 알려진 자격 증명이 있는 계정

2019년에 Google은 소비자 계정에 대한 연구를 통해 챌린지와 MFA가 자동화된 공격의 100%, 대량 피싱 공격의 96%, 표적 공격의 76%를 차단했다는 결과를 발표했습니다[5]. 이 비율은 공격이 발생한 것으로 알려진 일부 계정에 대해 계산된 것이므로 위의 수치와 직접 비교할 수는 없습니다.

저희는 2022년 4월부터 9월 사이에 비밀번호가 유출된 128,000개의 계정 샘플을 확보했습니다. 사용자에게 즉시 알림을 보냈습니다. 인증정보 유출이 발견되기 전 30일 동안 해당 계정을 소급하여 조사했습니다. 수동으로 계정을 검토한 결과, MFA가 있고 공격자가 비밀번호를 사용하여 보호된 리소스에 액세스하려고 시도한 것을 확인할 수 있는 7,861개의 계정을 발견했습니다. 이러한 계정의 경우 MFA가 공격의 98.6%를 차단한 것으로 나타났습니다.

이 샘플의 경우, 사용된 특정 유형의 MFA와 그 성능을 분석할 수 있었습니다. 자세한 결과는 표 2에 나와 있습니다. 5]와 마찬가지로 SMS는 다단계 인증용으로 특별히 설계된 모바일 애플리케이션인 Microsoft Authenticator보다 40.8% 더 효과적이지 않은 것으로 나타났습니다.

| **MFA 유형** | **실패율** |
|---|---|
| 인증 OTP | 0.99% |
| 인증자 알림 | 0.97% |
| SMS | 1.66% |
| **합계** | **1.44%** |

*표 2: 표 2: MFA 사용 및 미사용 결과*

# 결론

이번 연구에서는 상업용 계정을 보호하는 데 있어 다단계 인증(MFA)의 효과에 대한 첫 번째 분석을 실시했습니다. 벤치마크-승수 방법을 활용하고 유출 가능성이 있는 계정 샘플을 수동으로 검토한 결과, MFA를 설정한 계정의 99.99%가 조사 기간 내내 보호 상태를 유지한 것으로 나타났습니다. 또한, MFA를 구현하면 전체 집단에서 유출 위험이 99.22% 감소하고, 자격 증명에 다음과 같은 문제가 있는 경우에도 98.56% 감소하는 것으로 나타났습니다.

유출된 것으로 나타났습니다. 상업용 계정에 대한 이러한 결과는 소비자 계정에 대한 이전 연구에서 보고된 결과와 유사합니다.

또한, 저희 연구에 따르면 전용 MFA 애플리케이션이 SMS 기반 인증보다 성능이 우수하지만, 두 가지 방법 모두 MFA를 전혀 사용하지 않는 것보다 훨씬 더 효과적인 것으로 나타났습니다. 이러한 연구 결과에 비추어 볼 때, 이미 많은 기관에서 요구하고 있는 것처럼 사이버 보안 조치를 강화하기 위해 상업용 계정에서 MFA를 기본적으로 활성화할 것을 강력히 지지합니다[18].

# 참조

[1] 데이비드 맨델 프리먼, 삭시 자인, 마르쿠스 뒤르무스, 바티스타 비지오, 조르지오 지아신토. 당신은 누구입니까? 사용자 신뢰도 측정을 위한 통계적 접근법. *NDSS*, 16:21-24, 2016.

[2] L. O'Gorman. 사용자 인증을 위한 비밀번호, 토큰 및 생체 인식 비교. *url = https://slate.com/technology/2022/02/google-multifactor-authentication-effectiveresearch.html,ceedings of the IEEE*, 91(12):2021-2040, 2003.

[3] 아나스타시오스 리베레토스, 이보 드라가노프. 고객 ID 및 액세스 관리(CIAM): 주요 기술 공급업체 개요. *국제 경제 및 경영 시스템 저널*, 07, 2022.

[4] 산차리 다스, 앤드류 딩먼, L. 진 캠프. Johnny가 2단계 보안 키를 사용하지 않는 이유 FIDO U2F 보안 키에 대한 2단계 사용성 연구. 사라 마이클존과 카즈에 사코, 편집자, *금융 암호화 및 데이터 보안*, 10957권, 160-179쪽. 스프링거 베를린 하이델베르크, 2018.

[5] 페리윙클 도어플러, 커트 토마스, 마이야 마린첸코, 주리 라니에리, 유장, 안젤리카 모스키치, 데이먼 맥코이. 계정 탈취에 대한 방어 수단으로서 로그인 문제 평가하기. *월드 와이드 웹 컨퍼런스 - WWW '19*, 372-382페이지. ACM Press, 2019.

[6] 에밀리아노 드 크리스토파로, 홍루 두, 줄리앙 프로이디거, 그렉 노시에. 이중 인증의 비교 사용성 연구. http://arxiv.org/abs/1309.5344, 2014.

[7] 앤 애덤스와 안젤라 사세. 사용자는 적이 아닙니다. *ACM 커뮤니케이션*, 42:40-46, 1999.

[8] 에니스 울키나쿠, 다니엘 레인, 스드잔 카쿤. 2FA-PP: 2차 페이토르 피싱 방지. *제12회 무선 및 모바일 네트워크의 보안 및 개인정보 보호 컨퍼런스 논문집,* 60-70페이지. ACM, 2019.

[9] 조셉 보노, 코맥 헤일리, 폴 오어쇼트, 프랭크 스타자노. 비밀번호를 대체하기 위한 탐구: 웹 인증 체계의 비교 평가를 위한 프레임워크. 2012 *IEEE 보안 및 개인정보 보호 심포지엄*, 553-567페이지, 2012.

[10] 멀티팩터 인증이 예전보다 덜 효과적인가요?

https://slate.com/technology/2022/02/google-multifactor-authen- tication-effective-research.html, 2022.

[11] 멀티팩터 인증에 실패했나요? https://www.pcmag.com/news/has-multi-authentication-failed-us, 2023.

[12] Tarek Dawoud. Microsoft Azure Active Directory용 제로 트러스트 배포 가이드. https://www.microsoft.com/en-us/security/

blog/2020/04/30/zero-trust-deployment-guide-azureactive-directory/, 2020.

[13] 미셸 카스텔. 온라인 계정 탈취 완화: 교육 사례. *소매 결제 위험 포럼*, 2013.

[14] 매튜 히크먼과 콜린 테일러. 유병률을 추정하는 간접적 방법. 질리 슬로보다, 편집자, *약물 남용의 역학*, 113-131 페이지. 스프링거-베를라그, 2005.

[15] 라민 모즈타바이. 벤치마크 승수 방법을 사용하여 미국에서 약물 사용 장애의 유병률 추정. *JAMA 정신의학*, 79(11):1074, 2022.

[16] 카트제 볼라에르츠, 마크 에어츠, 안드레 사세. 벨기에에서 상습 약물 사용의 유병률을 추정하기 위한 개선된 벤치마크 승수 방법, 2000-10. *공중 보건 기록 보관소*, 71(1):10, 2013.

[17] Microsoft: 침해된 계정의 99.9%가 멀티팩터 인증을 사용하지 않았습니다. https://www.zdnet.com/article/microsoft-99-9-of-compromised-계정-did-not-use-multi-factorauthentication/, 2020.

[18] 아리엘 F. 폼푸티우스. 이중 인증에 대한 검토: 제안된 보안 노력이 의무로 전환됩니다. *의료 참조 서비스 분기별*, 37(4):397-402, 2018.

이 논문은 arXiv(https://arxiv.org/abs/2305.00945)에서도 볼 수 있습니다.