**Report** | August 2026


# RecruitTrap

## The Growing Threat of Browser-in-the-Browser (BitB) Recruitment Scams

Analysis by CTM360

CTM360®

**INDUSTRY** Recruitment

**COUNTRY** All

**REGION** Global

**DATE** August, 2026

**Threat Type** Phishing Campaign

**Threat Vector** Scam Email

**Key Techniques** BITB, Credential & OTP Harvesting

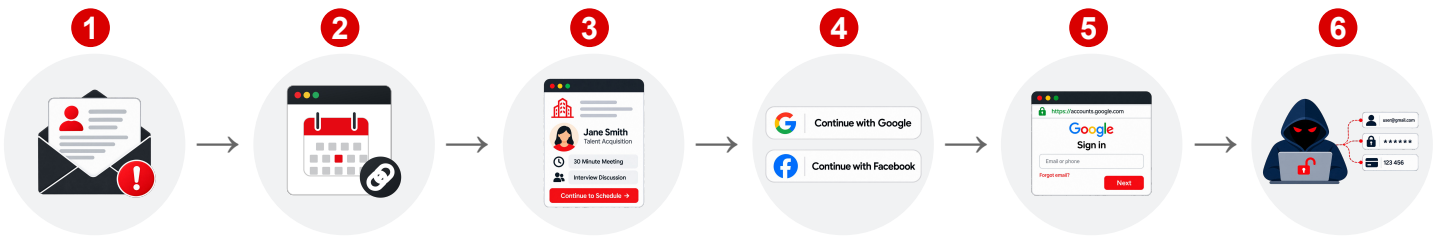
**Phishing Instances** 3000+ URLs

# Overview

CTM360 has identified a **large-scale, global Browser-in-the-Browser (BitB) recruitment-themed phishing campaign** targeting professionals, particularly individuals working in marketing and related roles. Threat actors impersonate recruiters from more than **50+ recognizable organizations** across technology, travel, hospitality, food and beverage, apparel, consulting, and entertainment. The campaign uses copied corporate branding, realistic hiring pages, and in some cases the **names and photographs of real recruiters** to make unsolicited interview invitations appear legitimate. **CTM360 have identified more than 3000+ URLS, over the last 2 months.** However, these findings likely represent only the tip of the iceberg. With scalable phishing kits and advanced techniques, the true volume of active BitB Recruitment scam URLs will be significantly higher.

The attack begins with a convincing recruiter email or meeting invitation. Victims are then directed through one of two primary workflows: a **brand-specific recruitment portal** or a **counterfeit Calendly-style scheduling page** where they select a date and time and provide basic contact details. This use of brand-specific recruitment portal helps the campaign appear legitimate and can reduce the effectiveness of link-based security controls.

Both BitB recruitment scam workflows ultimately prompt the victim to **"Continue with Google"** or **"Continue with Facebook."** Instead of opening a genuine authentication window, the phishing site renders a **Browser-in-the-Browser (BitB)** interface that visually reproduces the selected provider's login page, including a fake address bar and security indicators. Credentials and authentication data entered into this window are captured by the attacker. In more advanced BitB recruitment variants, the backend can dynamically relay credentials and MFA challenges in real time, enabling the threat actor to establish an authenticated session while the victim is still interacting with the phishing page.




**Recruitment Phishing Email**

The victim receives a scam recruitment email impersonating a known company, containing a "View Calendar Availability" or similar interview-scheduling link.

**Interview / Calendar Link**

The victim clicks the embedded calendar or interview link believing they are proceeding to a legitimate recruitment process.

**Fake Branded Meeting Page**

The victim lands on a fake scheduling page which may use a company branding and, in some cases, real recruiter details, before being prompted to authenticate.

**Continue with Google / Facebook**

The victim is prompted to continue using their Facebook or Google accounts presented on the fake meeting page.

**Browser-in-the-Browser (BitB) Login**

A fake BitB Google/Facebook login window appears, complete with a convincing address bar and authentication interface.

**Credential Theft & Account Compromise**

Credentials and PII entered into the counterfeit window are captured, enabling attempted unauthorized access to the victim's account.

CTM360®

# FRAUD STAGES:

## CTM360 Fraud Navigator

**PHASE 1**

Infrastructure & Delivery

**1 Resource Development**

- Hosting
  - Dedicated Hosting
  - Website Builder
  - Free Hosting
- Domain
  - Lookalike Domain
  - Subdomain
  - Dedicated Domain
- Phishing Kits
  - All-In-One Kits

**2 Trigger**

- Deceptive Incentives
  - Financial Incentive
  - Fake Offers
  - False Promise
- Social Engineering
  - Brand Impersonation
- Cognitive Pressure
  - Urgency

**3 Distribution**

- Peer-to-Peer
  - Email

**PHASE 2**

Victim Engagement & Fraud

**4 Target Interaction**

- Website
  - Impersonated website

**5 Motive**

- Credential Harvesting
  - OTP collection
  - Login information
- Account Hijacking
- PII harvesting
  - Login information
  - Email Account
  - Instant Messaging Account

**6 Monetization**

- Sale of Stolen Digital Assets

Stage (Tactic/Category)

Category

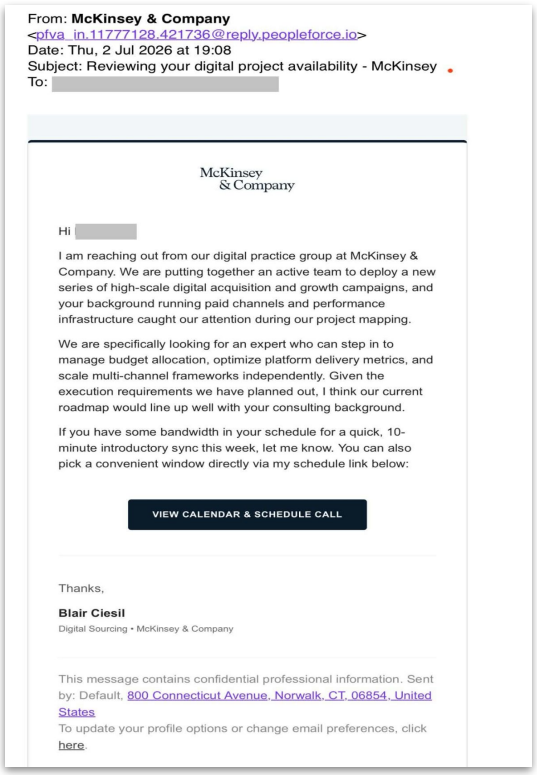
Technique

The Fraud Navigator framework has been mapped to show how it aligns with each stage of the newly identified scam variants. This helps highlight how the scams evolve across both phases.

# CTM360 Observation

## Recruitment Email & Recruiter Impersonation

The attack begins with targeted recruitment emails that appear to come from a legitimate recruiter at a well-known organization. The email references the recipient's background and invites them for an informal discussion or interview.



From: **McKinsey & Company**
<pfva_in.11777128.421736@reply.peopleforce.io>
Date: Thu, 2 Jul 2026 at 19:08
Subject: Reviewing your digital project availability - McKinsey
To: [redacted]

McKinsey & Company

Hi [redacted]

I am reaching out from our digital practice group at McKinsey & Company. We are putting together an active team to deploy a new series of high-scale digital acquisition and growth campaigns, and your background running paid channels and performance infrastructure caught our attention during our project mapping.

We are specifically looking for an expert who can step in to manage budget allocation, optimize platform delivery metrics, and scale multi-channel frameworks independently. Given the execution requirements we have planned out, I think our current roadmap would line up well with your consulting background.

If you have some bandwidth in your schedule for a quick, 10-minute introductory sync this week, let me know. You can also pick a convenient window directly via my schedule link below:

VIEW CALENDAR & SCHEDULE CALL

Thanks,

**Blair Ciesil**
Digital Sourcing • McKinsey & Company

This message contains confidential professional information. Sent by: Default, 800 Connecticut Avenue, Norwalk, CT, 06854, United States
To update your profile options or change email preferences, click here.

*Sample recruiter email impersonating McKinsey & Company Careers targeting Marketing Professionals*

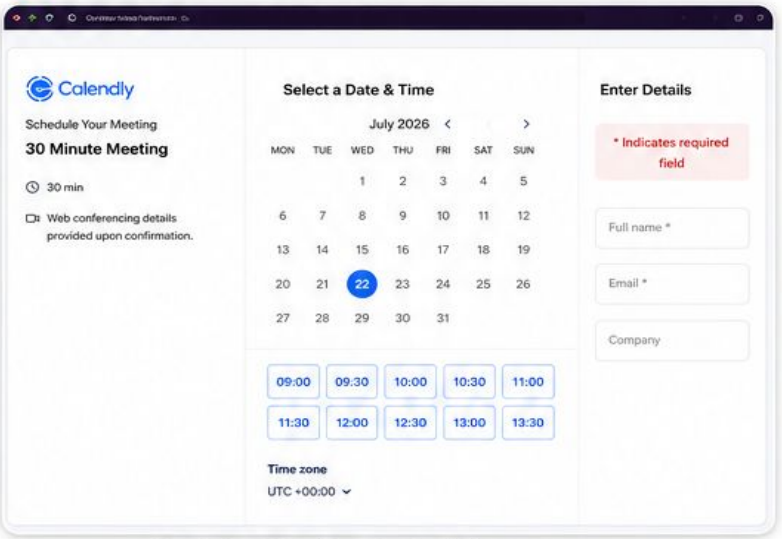
## Marketing Professionals as Primary Targets

Based on our analysis, we observed that majority of the BitB recruitment scam emails targeted marketing professionals. This targeting appears deliberate, as marketing professionals often have access to advertising platforms, corporate social media accounts, customer data, and other business-critical services, making their accounts particularly valuable to threat actors.

## Counterfeit Brand Recruitment & Calendly-Style Scheduling Portals

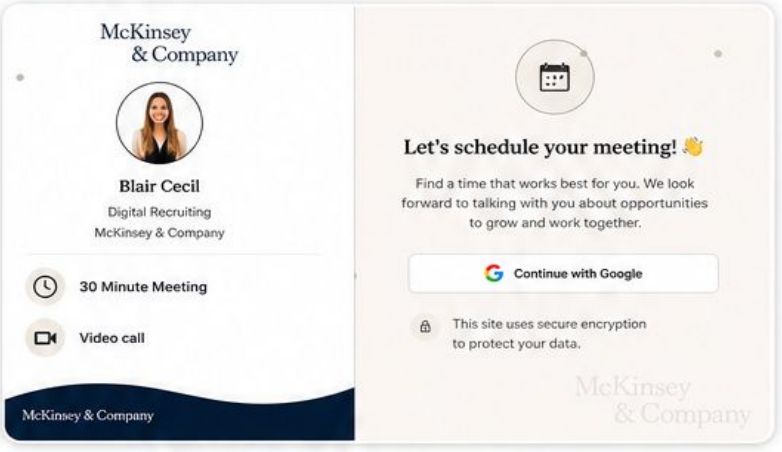
The BitB recruitment scam uses two main phishing kits: **Counterfeit Calendly-style scheduling pages** and **brand-specific recruitment portals.** The Calendly-style pages ask victims to schedule an interview and enter basic contact details, while the brand-specific recruitment portals impersonate real companies using real recruiters names, photos, job titles, and branding. These realistic elements make the scam appear more legitimate and harder to detect. Both include **"Continue with Google/Facebook"** login buttons that open a BitB phishing window targeting the either Google or Facebook credentials.

### A Calendly-Style Scheduling Portal




Fraudulent Calendly-style scheduling page.

### B Brand-Specific Recruitment Portal



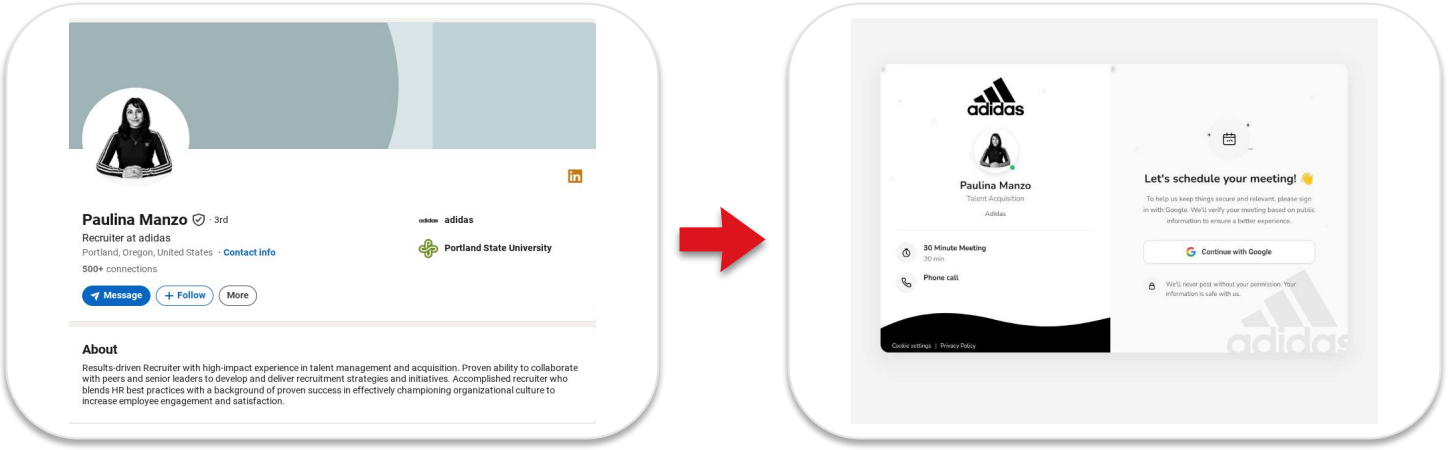

Fraudulent brand-specific recruitment portal.

# Abuse of Recruiter Identities & Corporate Branding

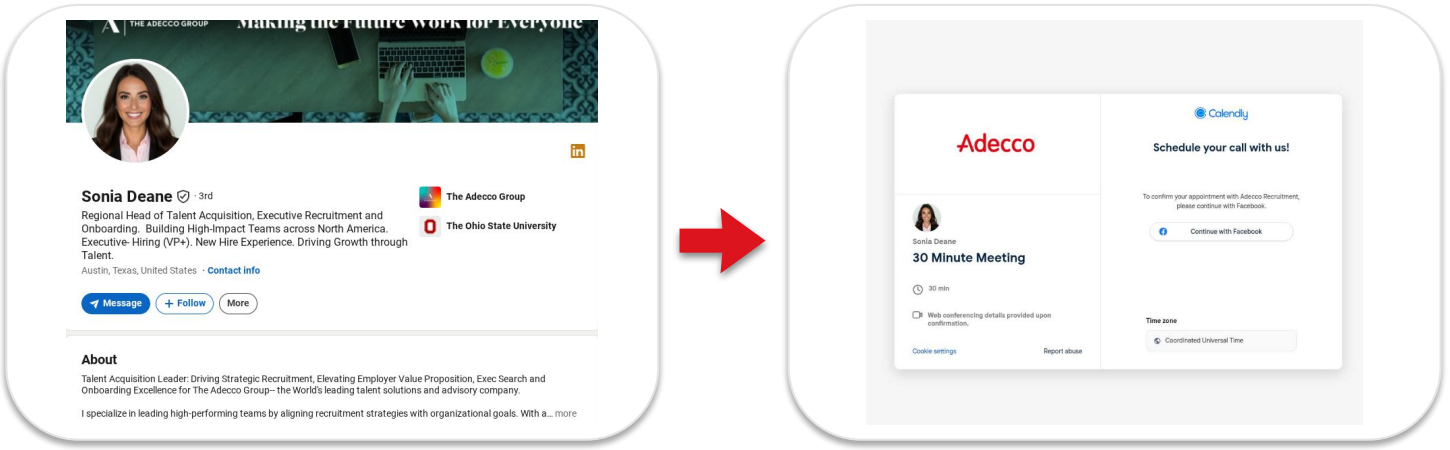
Our analysis identified multiple instances in which threat actors leveraged publicly available information associated with legitimate recruiters to enhance the credibility of fraudulent recruitment pages. These pages reused real recruiters names, profile images, job titles, employer information, and corporate branding to make attacker-controlled interview scheduling pages appear authentic and trustworthy.

| REAL RECRUITER PROFILE | FRAUDULENT RECRUITMENT PAGE |
|---|---|

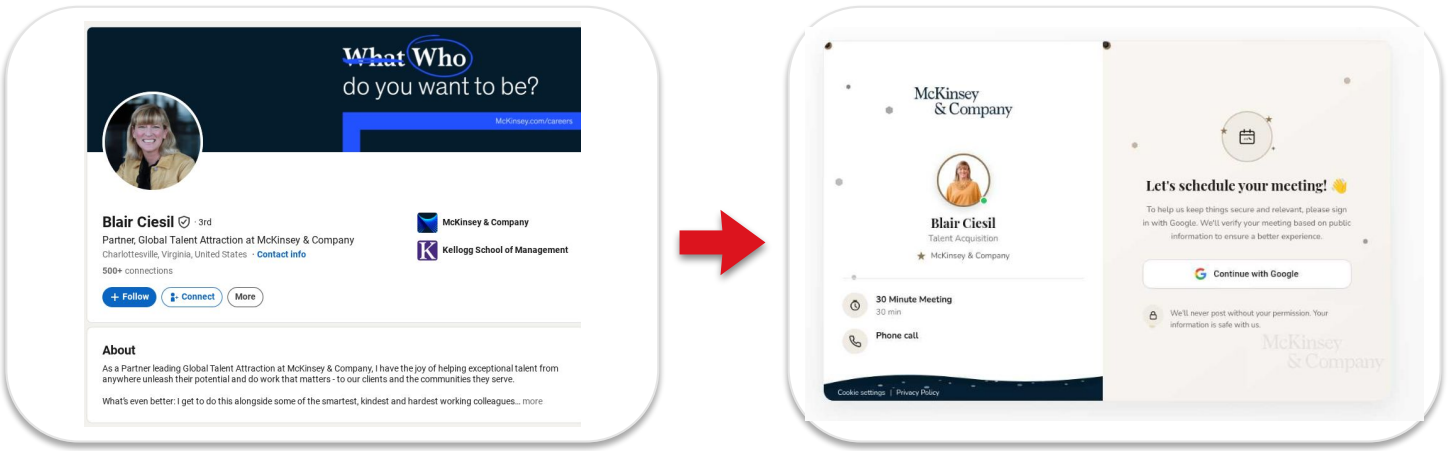
### ADIDAS — PAULINA MANZO




### McKINSEY & COMPANY — BLAIR CIESIL




### ADECCO — SONIA DEANE



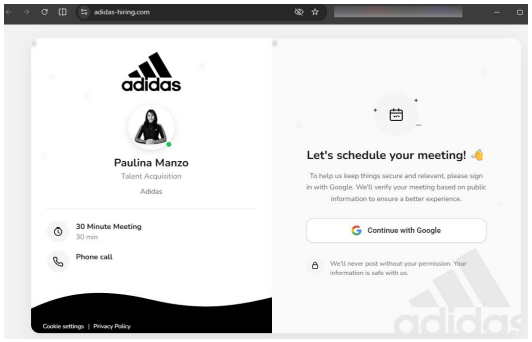

The repeated use of this approach across multiple organizations shows that the same recruitment scam can be easily adapted to impersonate different recruiters and brands.

# Two Entry Paths, Same BitB Destination

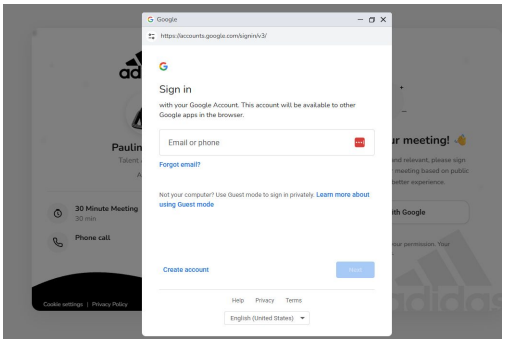
Both the counterfeit **Calendly-style scheduling pages** and **brand-specific recruitment portals** begin with an email or meeting lure. Victims are then directed either to a fake recruitment portal or a Calendly-style booking flow. In both cases, the process leads to a **Google or Facebook BitB phishing window**. The diagrams below illustrate how each scam flow works.

## A. COUNTERFEIT RECRUITMENT PORTAL FLOW

1. **Email lure** — Recruiter + brand
2. **Career portal** — Meeting prompt
3. **Provider Login button** — Google / Facebook
4. **BitB login** — Fake browser
5. **Credential theft** — Account takeover



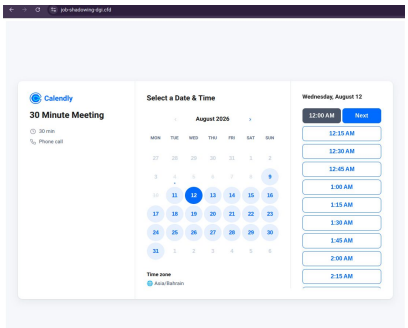

*Brand-specific meeting portal*



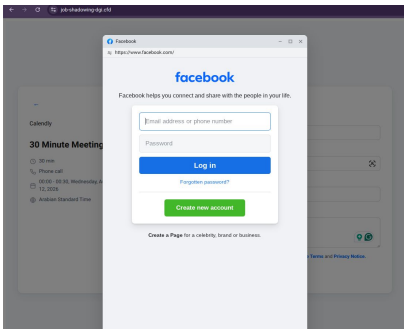

*Google BitB after provider selection*

## B. CALENDLY-STYLE SCHEDULING FLOW

1. **Email / link** — Meeting invitation
2. **Date & time** — Select a slot
3. **Applicant details** — Name / email / phone
4. **BitB login** — Google / Facebook
5. **Credential theft** — Account Takeover




*Calendly-style date and time selection*



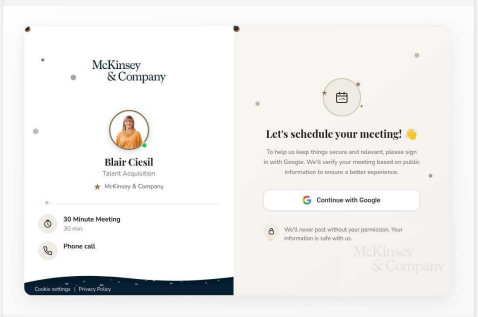

*Facebook BitB after scheduling details*

### Mobile-Specific Phishing Behavior

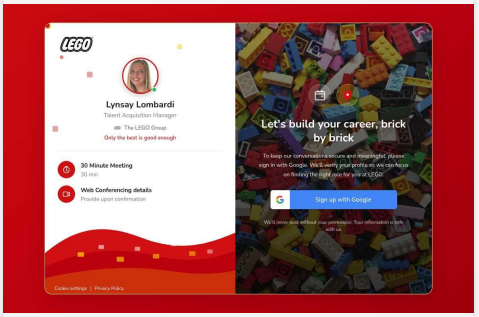
We observed that when the phishing link is opened on a mobile device, the campaign may display a full-screen fake Google or Facebook login page instead of using a BitB window. Making the phishing page appear like a normal mobile login screen.

# Recruitment-Themed Templates - Sample Set

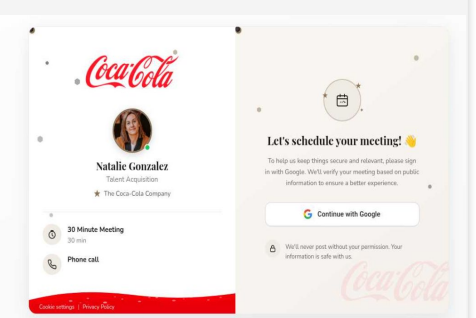
The same template has been reused by the threat actor by replacing the brand, recruiter persona, background, slogan and provider button while retaining the same 30 minute meeting and authentication flow.



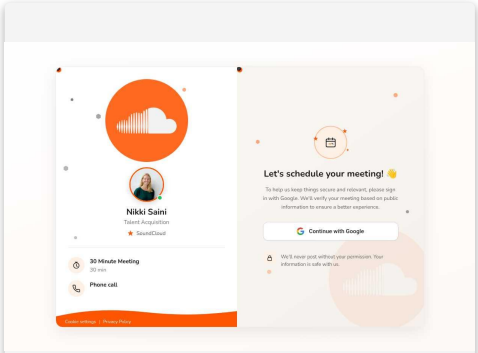

*McKinsey & Company - Google BitB*



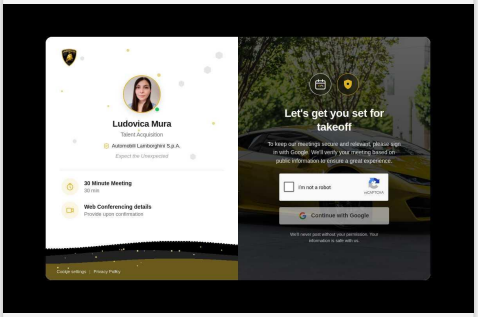

*LEGO - Google BitB*



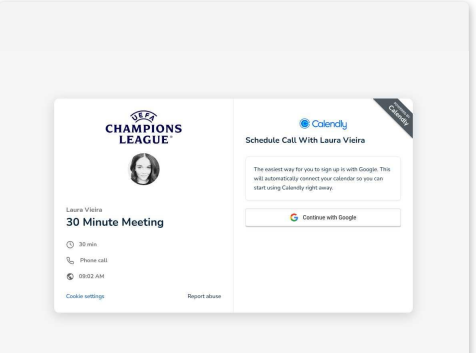

*Coca Cola - Google BitB*



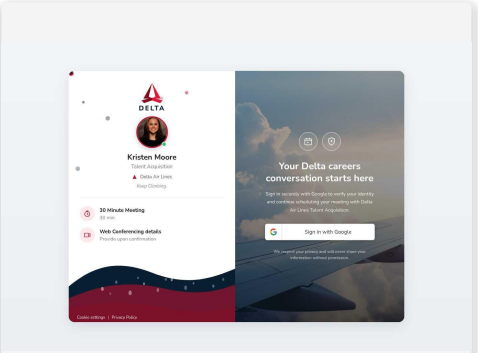

*SoundCloud*



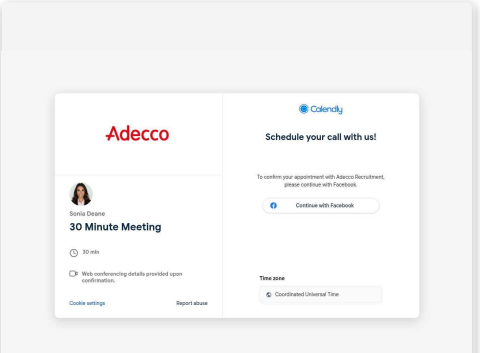

*Account Verification Scam*



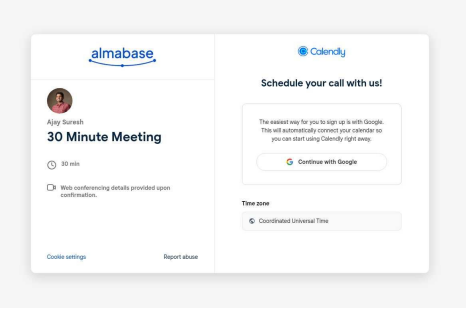

*Champions League*




*Delta - Google BitB*




*Adecoo - Facebook BitB*

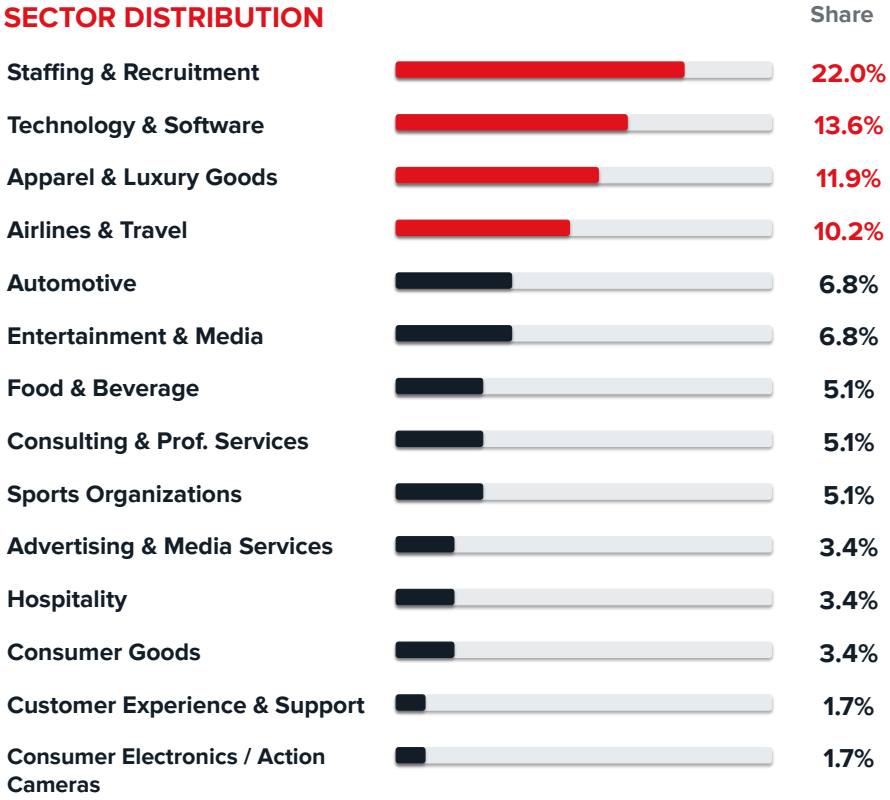



*AlmaBase - Google BitB*

# Targeted Brands & Sectors

The recruitment-themed Browser-in-the-Browser (BitB) campaign demonstrates broad and diverse brand targeting, with **50+ organizations identified across 10+ sectors**.

## SECTOR DISTRIBUTION




**58%**

**of named brands sit in the top four sectors**

Staffing, technology, apparel/luxury, and travel drive the majority of brand exposure.

## REPRESENTATIVE BRANDS TARGETED

| | |
|---|---|
| **Staffing** | Adecco · Randstad · ManpowerGroup · Hays · Kelly · Aquent · Creative Circle · Almabase |
| **Tech** | Apple · NVIDIA · OpenAI · Adobe · SAP · Epic Games · Criteo · Greenhouse |
| **Apparel** | Nike · Adidas · Louis Vuitton · Hermès · Tiffany & Co. · Cartier · Levi's |
| **Travel** | Delta · Emirates · American Airlines · United Airlines · Expedia · Booking.com |

As shown above, the most targeted sector is **Staffing & Recruitment**, with **13 brands**. This is followed by **Technology & Software** with **8 brands, Apparel & Luxury Goods** with **7 brands, and Airlines & Travel** with **6 brands.** Together, these four sectors make up around **58% of all identified brands**. This shows that threat actors are using well-known companies and recruitment brands to make fake job offers and interview invitations look more real and trustworthy.

In addition to these top sectors, the campaign also targets brands from many other sectors, including **automotive, entertainment and media, food and beverage, consulting and professional services, sports organizations, advertising and media services, hospitality, consumer goods, Customer Experience & Support, and consumer electronics**. This shows that the campaign is not focused on one type of company or industry and can be used against a wide range of brands.

The campaign can also be **easily changed to target different brands**. Threat actors can use the same recruitment phishing setup and simply change the company name, logo, recruiter details, and other content. This allows them to target different companies, industries, and users without having to create a completely new campaign each time.

## Key Takeaway

The campaign targets **many well known brands across different sectors** and can be easily changed to impersonate new organizations. By using trusted company names and realistic recruitment messages, threat actors can make their fake job and interview offers appear more convincing.

# Recruitment-Phishing Infrastructure

Over the last 2 months CTM360 has detected over **3,000+** Recruitment BitB URLs and identified Calendly as the primary target, accounting for about **95.8%** of the total observations, while the remaining activity impersonated multiple employer brands. Calendly-targeting pages were predominantly protected by Cloudflare, which concealed their origin servers, while employer-brand impersonation pages relied on dedicated lookalike domains that reused AWS-hosted IP addresses and recurring hostname structures indicating that multiple phishing sites were deployed through shared infrastructure.

**3000+**

**PHISHING URLs DETECTED**

Recruitment BitB dataset · last 2 months

## SAMPLE OBSERVED PHISHING URLs (IOCs)

Five examples from each dataset

| COUNTERFEIT CALENDLY-STYLE | COUNTERFEIT RECRUITMENT PORTAL |
|---|---|
| hxxps[:]//discover[.]hremployment-pub[.]com | hxxps[:]//deltaairlines-global[.]com |
| hxxps[:]//inside[.]talentforgejourney-pub[.]works | hxxps[:]//flyemirates-global[.]com |
| hxxps[:]//world[.]applicantinterview-pub[.]com | hxxps[:]//deloitte-careers[.]com |
| hxxps[:]//media[.]interviewconfirmation[.]info | hxxps[:]//legohr-careers[.]com |
| hxxps[:]//zone[.]interviewschedule[.]cfd | hxxps[:]//expedia-careers[.]com |

## PAGE-TITLE PATTERN FINDINGS

Recurring page titles across 3,000+ valid BitB Recruitment scams

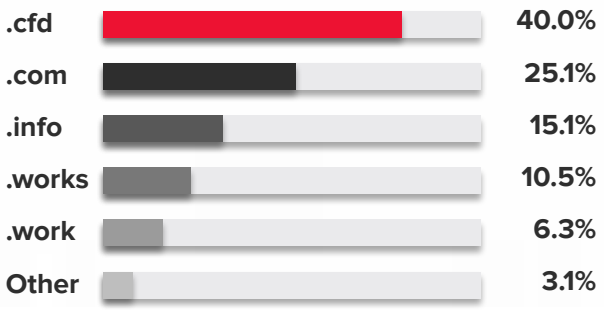
| PAGES | OBSERVED PATTERN |
|---|---|
| 846 | **Exact title reuse** "Job Search \| Calendly Careers" |
| 913 | **Employment-title family** Job / Career / Recruitment |
| 295 | **Booking-action cue** "Select a Date & Time" titles |

**WHY IT WORKS**

Page titles show recruiting and Calendly booking lures dominate.

## TLDS USED IN THE CAMPAIGN

Share of 813 deduplicated registered domains




.cfd represented the largest observed TLD share (40.0%).

## HOSTING INFRASTRUCTURE

All 3,000+ URL incidents are retained. Percentages below use unique observed hosts within each page type.

### CALENDLY-TARGETING INFRASTRUCTURE

928 unique observed hosts

**92.2%**
Cloudflare-fronted BitB hosts

**7.7%**
Direct / dedicated IP hosts

Predominantly Cloudflare-fronted phishing infrastructure targeting Calendly.

### EMPLOYER-BRAND INFRASTRUCTURE

116 unique observed hosts

**93.1%**
Dedicated / registered hosts

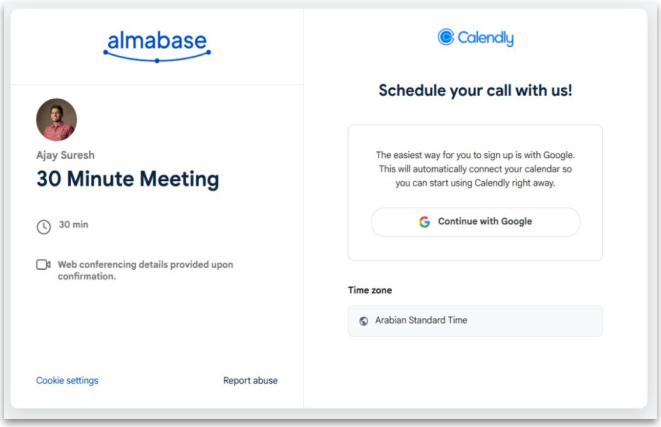
**50.9%**
Hosted on AWS EC2 IPs & ranges

Employer brand lookalike domains use dedicated infrastructure with recurring AWS hosting.

# Technical Breakdown: BITB & Live AiTM Workflow

## Investigation Brief

As part of our investigation into the recruitment-themed phishing campaign, our team has analyzed one of the Calendly-style BitB Phishing URL.




*UI of the Recruit Trap BitB phishing page being analyzed.*

By examining the site's frontend code and client-side behavior, we were able to identify how victims are filtered, how Google-style login and multi-factor authentication prompts are reproduced, how credentials and MFA information are captured, and how the browser communicates with the backend infrastructure. The following technical analysis documents these behaviors and explains how the site supports a real-time phishing workflow targeting business users.

**Assessment**

Architecture is consistent with real-time adversary-in-the-middle phishing: the backend can interactively collect credentials, request MFA codes or push confirmations, and then redirect victims into a legitimate Calendly workflow to reduce suspicion.

## Observed Frontend Pattern

The page behaves as a state machine rather than a static form.

```
scenes = [
  CAPTCHA, LOGIN, PASSWORD,
  TWO_FACTOR_CODE,
  TWO_FACTOR_PHONE,
  TWO_FACTOR_NUMBER_MATCH,
  TWO_FACTOR_SUFFIX, DONE
]

sessionStorage.sid = browserId
socket.on('scene', renderStage)
```

### Technical signals

- Svelte/SvelteKit front end controls staged prompts.
- Per-browser session identifier persists in sessionStorage.
- CAPTCHA and browser-reload checks filter victims before collection.

## Backend-Controlled Flow

Persistent **Socket.IO c**hannel lets the threat actor conduct the BitB Recruitment scam in real time.

1. **Session setup**
   Victim receives a browser-scoped session ID; CAPTCHA/reload filters reduce noise.
2. **Credential capture**
   Email, password, and geolocation data are transmitted to the /api/login endpoint through a Google/Facebook-style authentication flow.
3. **Live Google login**
   The backend replays the credentials against Google and receives the required authentication type.
4. **MFA relay**
   The phishing page renders the matching MFA prompt and forwards OTP/SMS/email codes to /api/twofa or related endpoints.
5. **Session takeover**
   The attacker is granted an authenticated session; the victim is then redirected to a genuine page to reduce suspicion.

**Credential theft becomes interactive rather than one-shot**

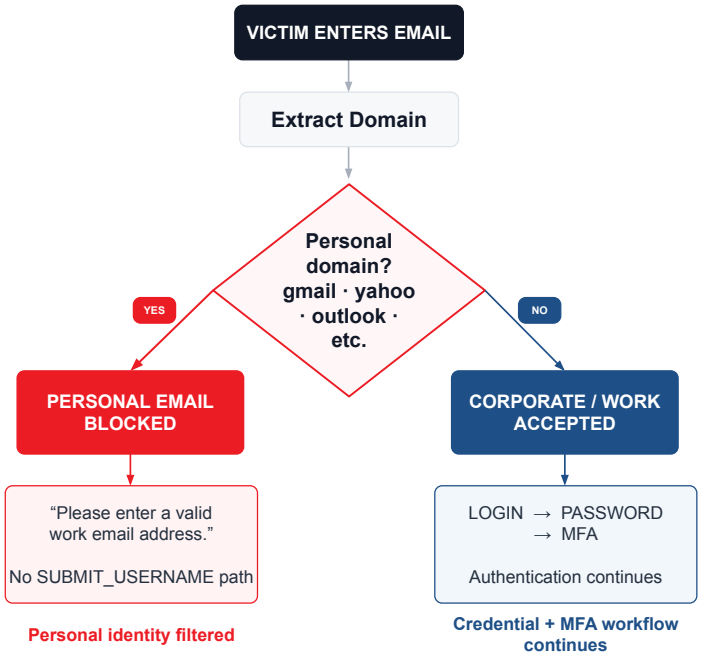
# Target Filtering: Corporate Email Qualification

The phishing site does not accept every victim: it first filters for potential corporate identities, then routes qualifying victims into the credential and MFA workflow.

## Victim-Qualification Flow

OBSERVED

Frontend gates the authentication path by domain category before submitting the username.




## Analytical Assessment

INFERENCE

**Why filter personal email?**

- Enterprise identities may unlock corporate mail, documents and cloud resources.
- Compromised business mailboxes can expose trusted organizational contacts.
- Corporate accounts may reach SSO-connected applications.
- Business identities can enable follow-on phishing or BEC.
- The recruitment lure is more valuable when tied to a work identity.

## Observed Frontend Filtering Logic

CODE

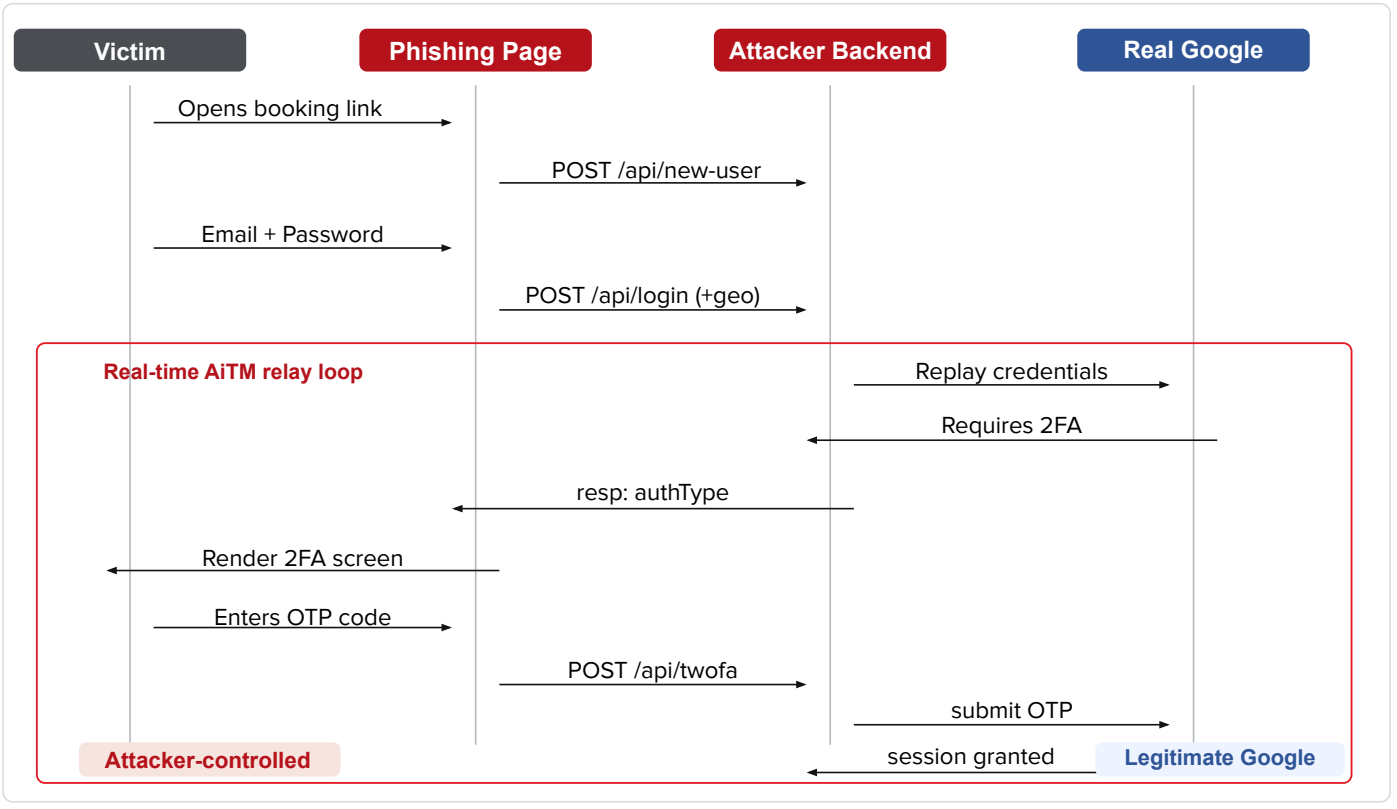
```
const domain =
  email.split("@")[1].trim().toLowerCase();

return !personalDomains.includes(domain);
```

**Blocked examples:** gmail.com · yahoo.com · outlook.com · icloud.com · protonmail.com

# Real-Time AiTM: Account Takeover

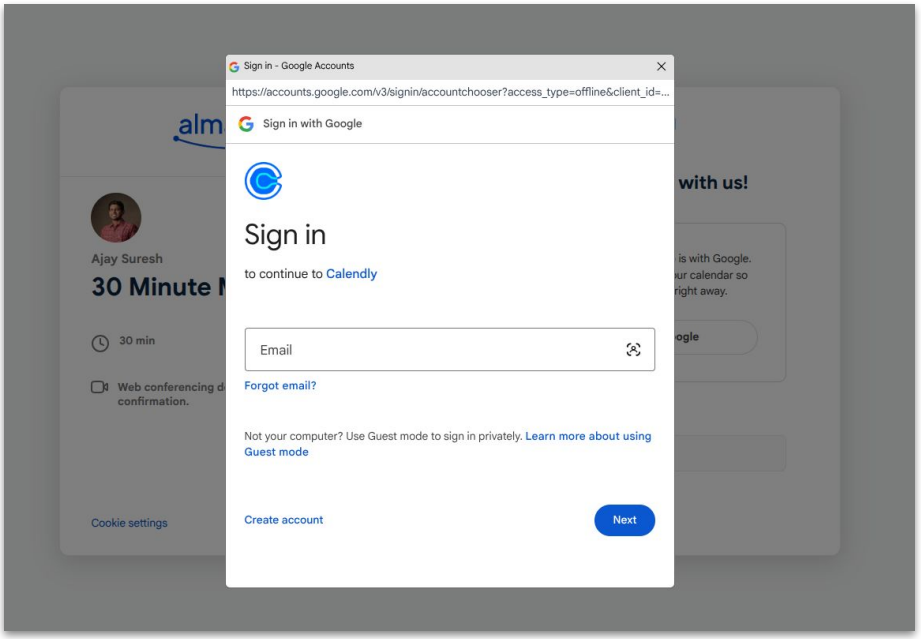
The advanced backend synchronizes the victim, phishing page, attacker session, and real Google authentication flow in real time.




*Observed credential and MFA relay workflow.*

# Browser-in-the-Browser Credential Theft

A fake browser window is rendered inside the phishing page to imitate Google authentication while the victim remains on the attacker-controlled origin.




*Fake Google sign-in popup drawn inside the malicious recruitment page.*

## Detection Clues

- The “window” cannot move outside the current browser tab.
- The visible Google address bar is part of the page, not browser chrome.
- Password managers may not recognize or autofill the expected Google origin.
- Buttons, privacy links, and browser controls may be decorative or non-functional.
- Credentials are posted to attacker-controlled endpoints rather than Google.

## Genuine vs. Counterfeit Authentication

### Genuine Google Sign-In

- Runs on accounts.google.com or another verified Google origin.
- Controlled by the browser or operating system.
- Passkeys and WebAuthn are bound to the legitimate site origin.

### BitB Sign-In Window

- Rendered as HTML/CSS within a lookalike recruitment page.
- Address bar, padlock, and window controls are only visual elements.
- Entered credentials can be captured immediately by the phishing frontend.

### Important distinction

BitB is the visual deception layer. Real-time MFA defeat requires a separate attacker backend that logs into the legitimate service and relays the requested second factor while the victim is still interacting with the phishing page.


## ABOUT US

CTM360 provides a consolidated platform that includes external attack surface management, digital risk protection (brand protection & anti-phishing, data leakage protection, and fully managed unlimited takedowns), security ratings, third party risk management, email intelligence (dmarc) and cyber threat intelligence.

## CONTACT US:

+973 77 360 360

info@ctm360.com

www.ctm360.com

21st Floor, East Tower Bahrain Financial  Harbour, Kingdom of Bahrain



CTM360®

**Mapping the World's External Digital Risks**

External | Consolidated | Technology, Data & Managed Services