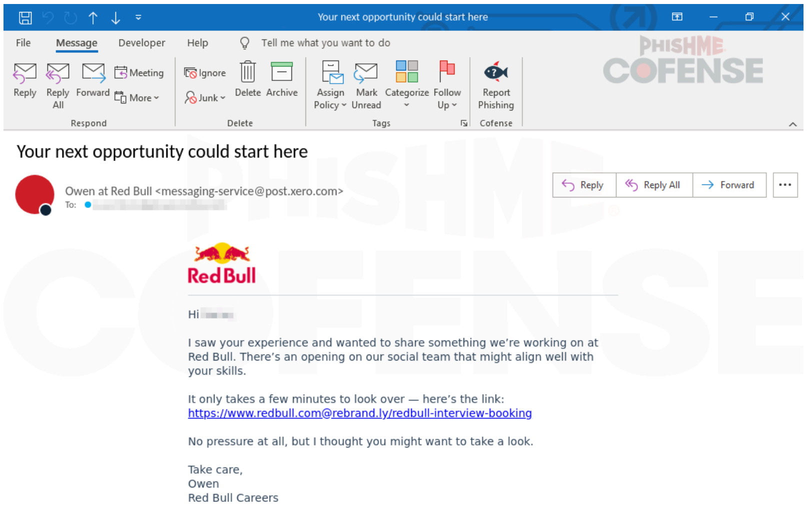
cofense.com /blog/phishing-from-home-the-hidden-danger-in-remote-jobs

Phishing from Home – The Hidden Danger in Remote Jobs Lurking in Tesla, Google, Ferrari, and Glassdoor

Phishing from Home –
The Hidden Danger in Remote Jobs Lurking in Tesla, Google, Ferrari, and Glassdoor
Monday
PHISHME
COFENSE

By: Emmett Smith and Brooke McLain, Cofense Phishing Defense Center

In Q3 2024, the Cofense Phishing Defense Center (PDC) identified a phishing campaign that impersonated several Fortune 500 companies by targeting individuals in social media and marketing positions through fake job applications. Earlier this year, the team researched how resume details have become valuable tools for threat actors in a blog titled “Job Application Spear Phishing.” Since then, the PDC has continued to monitor the use of this tactic by threat actors who have begun utilizing other well-known brands as well as refining their techniques to further deceive potential victims.



Your next opportunity could start here

Owen at Red Bull <messaging-service@post.xero.com>
To: [redacted]

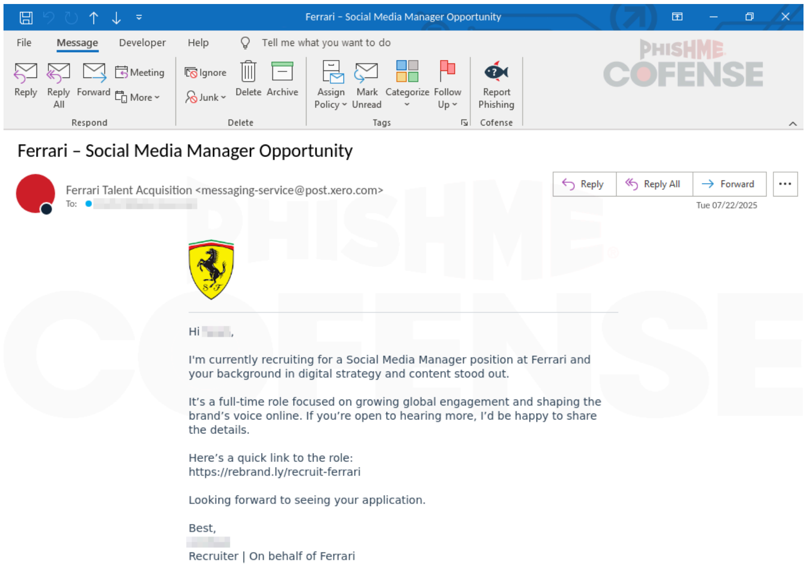
Hi [redacted]

I saw your experience and wanted to share something we’re working on at Red Bull. There’s an opening on our social team that might align well with your skills.

It only takes a few minutes to look over — here’s the link:
https://www.redbull.com@rebrand.ly/redbull-interview-booking

No pressure at all, but I thought you might want to take a look.

Take care,
Owen
Red Bull Careers



Ferrari – Social Media Manager Opportunity

Ferrari Talent Acquisition <messaging-service@post.xero.com>
To: [redacted]
Tue 07/22/2025

Hi [redacted],

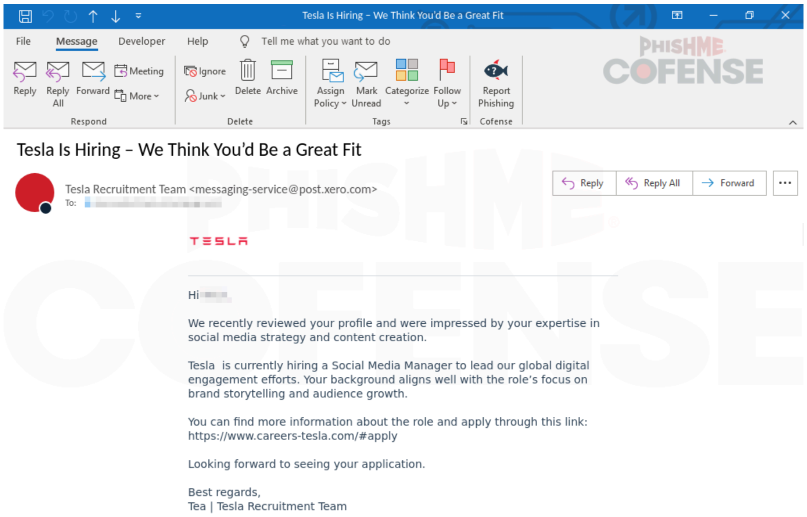
I'm currently recruiting for a Social Media Manager position at Ferrari and your background in digital strategy and content stood out.

It’s a full-time role focused on growing global engagement and shaping the brand’s voice online. If you’re open to hearing more, I’d be happy to share the details.

Here’s a quick link to the role:
https://rebrand.ly/recruit-ferrari

Looking forward to seeing your application.

Best,
[redacted]
Recruiter | On behalf of Ferrari



Tesla Is Hiring – We Think You'd Be a Great Fit

Tesla Recruitment Team <messaging-service@post.xero.com>
To: [redacted]

TESLA

Hi [redacted]

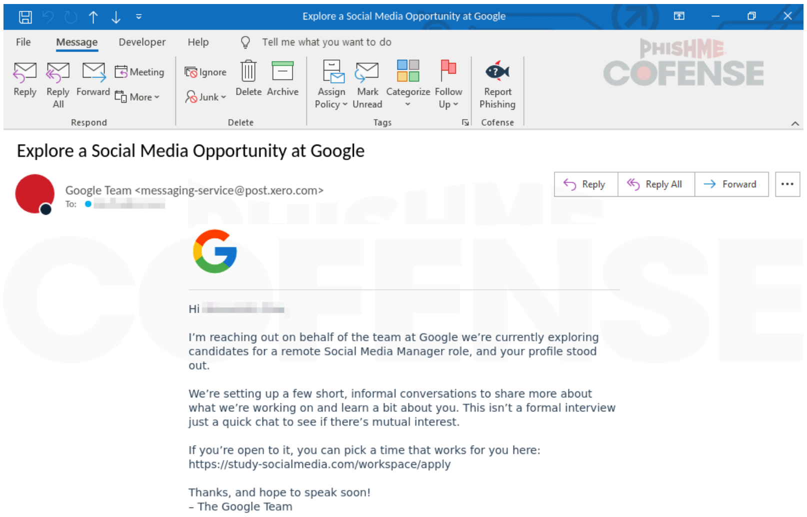
We recently reviewed your profile and were impressed by your expertise in social media strategy and content creation.

Tesla is currently hiring a Social Media Manager to lead our global digital engagement efforts. Your background aligns well with the role's focus on brand storytelling and audience growth.

You can find more information about the role and apply through this link:
https://www.careers-tesla.com/#apply

Looking forward to seeing your application.

Best regards,
Tea | Tesla Recruitment Team



Explore a Social Media Opportunity at Google

Google Team <messaging-service@post.xero.com>
To: [redacted]

Hi [redacted]

I'm reaching out on behalf of the team at Google we're currently exploring candidates for a remote Social Media Manager role, and your profile stood out.

We're setting up a few short, informal conversations to share more about what we're working on and learn a bit about you. This isn't a formal interview just a quick chat to see if there's mutual interest.

If you're open to it, you can pick a time that works for you here:
https://study-socialmedia.com/workspace/apply

Thanks, and hope to speak soon!
– The Google Team

Figure 1-4: Four Big Branded Emails (Red Bull, Tesla, Google, Ferrari)

Email Body Analysis

The email body, like the ones mentioned in the previous blog post, baits the candidate with an opportunity to apply to well-respected companies (Red Bull, Google, Tesla, and Ferrari) as seen above in Figures 1-4. The threat actors use specific phrasing, such as "No pressure at all, but I thought you might want to take a look," making the candidate more likely to learn more about this opportunity.

Another way the threat actor made this attack seem more legitimate was by spoofing various brand names while using "messaging-service[@]post.xero[.]com" as the from address. While Xero itself is a legitimate company, cybercriminals have exploited its email infrastructure in past phishing campaigns. By leveraging a trusted domain, attackers increase the likelihood of bypassing security filters and gaining the recipient's trust.

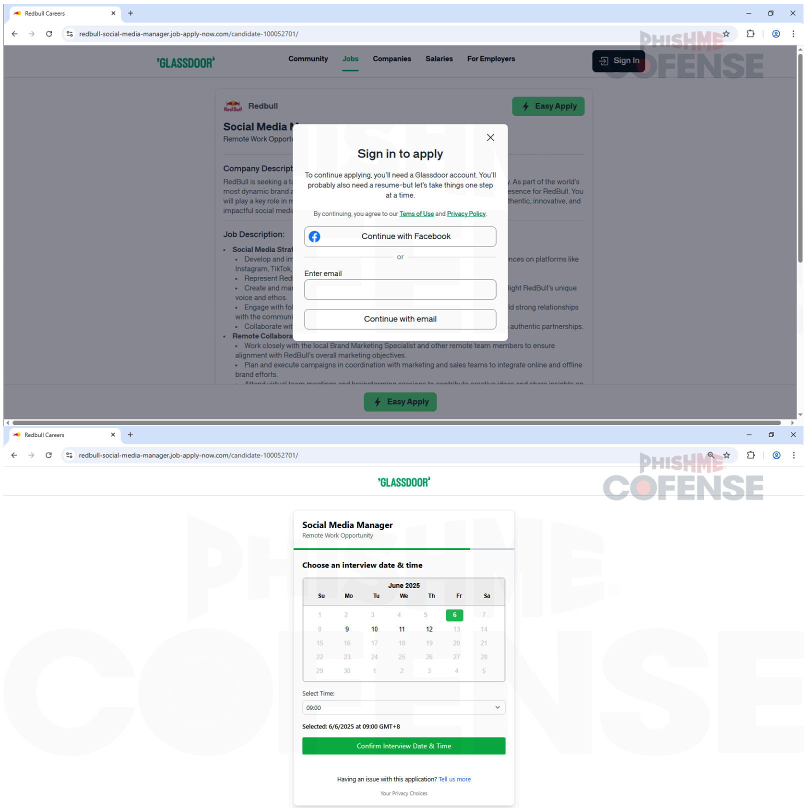
Phishing Page Analysis

The threat actor tailors the initial URLs to each brand by using their name within the subdomain of the URL, furthering the likelihood of the candidate clicking the link. The use of up-to-date images and logos for the login pages also gives the victim a false sense of legitimacy.

The Red Bull phishing campaign follows a similar path as previously seen by Cofense, beginning with a CAPTCHA page, then a false Glassdoor landing page that prompts users to either enter their email credentials or log in through a spoofed Facebook portal designed to harvest Facebook login information.

Tesla and Ferrari use a similar path as Red Bull, but instead of redirecting to a Glassdoor landing page, they lead to a fake Facebook login page. The Tesla phish landing page has a "Thank You" message, the role the candidate is applying for, and two options to sign in. Candidates can either choose to login with their Facebook credentials or with their email address. If the email option is chosen, it goes through a few steps and then leads back to the fake Facebook login.

The Google phishing email campaign employs an alternative method. Once a user submits their email address, they are redirected to a counterfeit "X" login page, which presents other credential entry options like Google or Apple.



redbull-social-media-manager.job-apply-now.com/candidate-100052701/

Sign in to apply

To continue applying, you'll need a Glassdoor account. You'll probably also need a resume-but let's take things one step at a time.

By continuing, you agree to our Terms of Use and Privacy Policy.

Continue with Facebook

or

Enter email

Continue with email

- Work closely with the local Brand Marketing Specialist and other remote team members to ensure alignment with RedBull's overall marketing objectives.
- Plan and execute campaigns in coordination with marketing and sales teams to integrate online and offline brand efforts.

redbull-social-media-manager.job-apply-now.com/candidate-100052701/

Social Media Manager

Remote Work Opportunity

Choose an interview date & time

June 2025

Su	Mo	Tu	We	Th	Fr	Sa
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	1	2	3	4	5

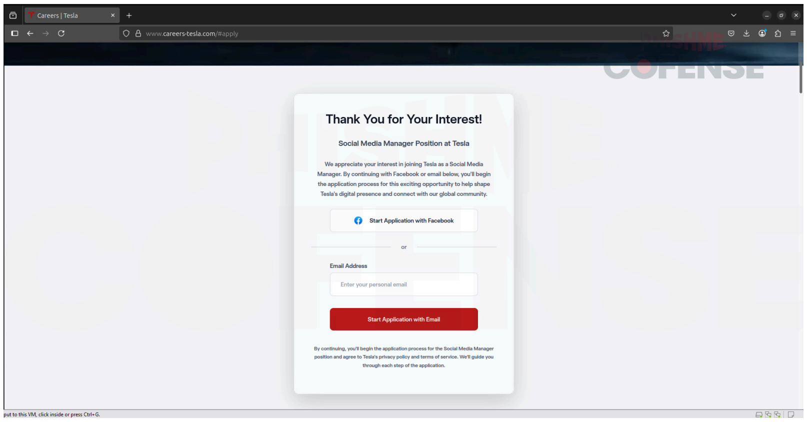
Select Time: 09:00

Selected: 6/6/2025 at 09:00 GMT+8

Confirm Interview Date & Time

Having an issue with this application? Tell us more

Your Privacy Choices



Thank You for Your Interest!

Social Media Manager Position at Tesla

We appreciate your interest in joining Tesla as a Social Media Manager. By continuing with Facebook or email below, you'll begin the application process for this exciting opportunity to help shape Tesla's digital presence and connect with our global community.

Start Application with Facebook

or

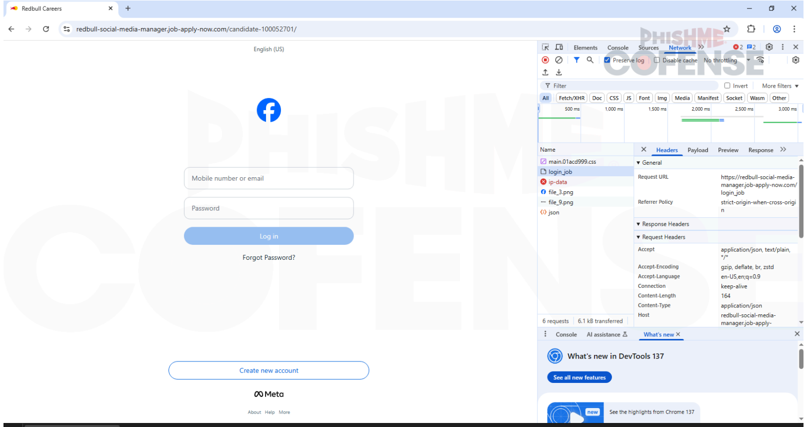
Email Address

Enter your personal email

Start Application with Email

By continuing, you'll begin the application process for the Social Media Manager position and agree to Tesla's privacy policy and terms of service. We'll guide you through each step of the application.

Figure 5-7: Easy Apply Button & Login Overlay



English (US)

Mobile number or email

Password

Log in

Forgot Password?

Create new account

Meta

About Help More

Name
main.01acd999.css
login_job
ip-data
file_3.png
file_9.png
json

6 requests 6.1 kB transferred

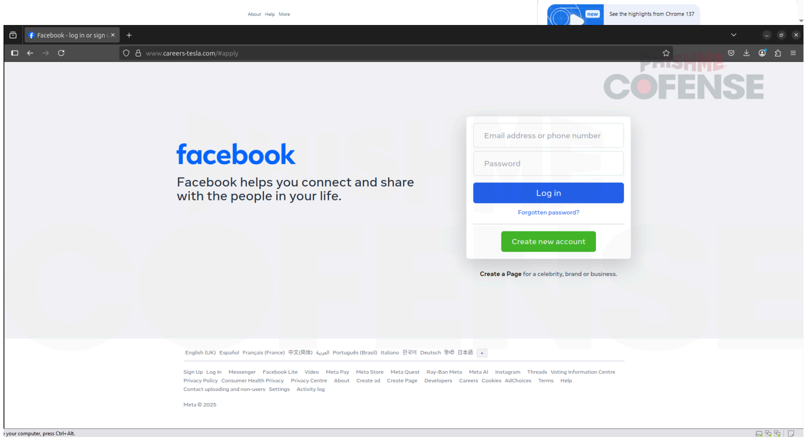
General

Request URL https://redbull-social-media-manager.job-apply-now.com/login_job
Referrer Policy strict-origin-when-cross-origin

Response Headers

Request Headers

Accept application/json, text/plain, */*
Accept-Encoding gzip, deflate, br, zstd
Accept-Language en-US,en;q=0.9
Connection keep-alive
Content-Length 164
Content-Type application/json
Host redbull-social-media-manager.job-apply-



facebook

Facebook helps you connect and share with the people in your life.

Email address or phone number

Password

Log in

Forgotten password?

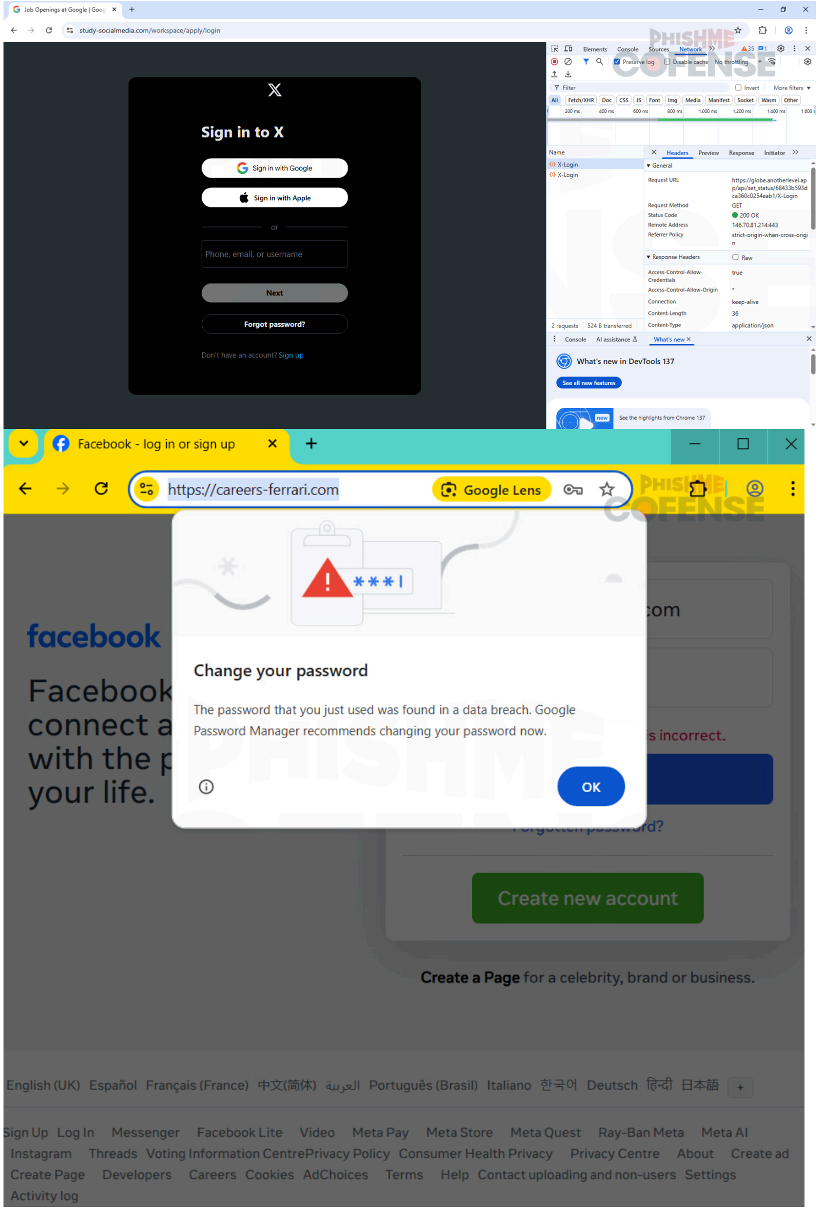
Create new account

Create a Page for a celebrity, brand or business.

English (UK) Español Français (France) 中文(简体) العربية Português (Brasil) Italiano 한국어 Deutsch हिन्दी 日本語 +

Sign Up Log In Messenger Facebook Lite Video Meta Pay Meta Store Meta Quest Ray-Ban Meta Meta AI Instagram Threads Voting Information Centre
Privacy Policy Consumer Health Privacy Privacy Centre About Create ad Create Page Developers Careers Cookies AdChoices Terms Help
Contact uploading and non-users Settings Activity log

Meta © 2025



study-socialmedia.com/workspace/apply/login

Sign in to X

Request URL: https://globe.anotherlevel.app/api/set_status/68433b593dca360c0254eab1/X-Login
Request Method: GET
Status Code: 200 OK
Remote Address: 146.70.81.214:443
Referrer Policy: strict-origin-when-cross-origin

Response Headers
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: *
Connection: keep-alive
Content-Length: 36
Content-Type: application/json

https://careers-ferrari.com

Change your password

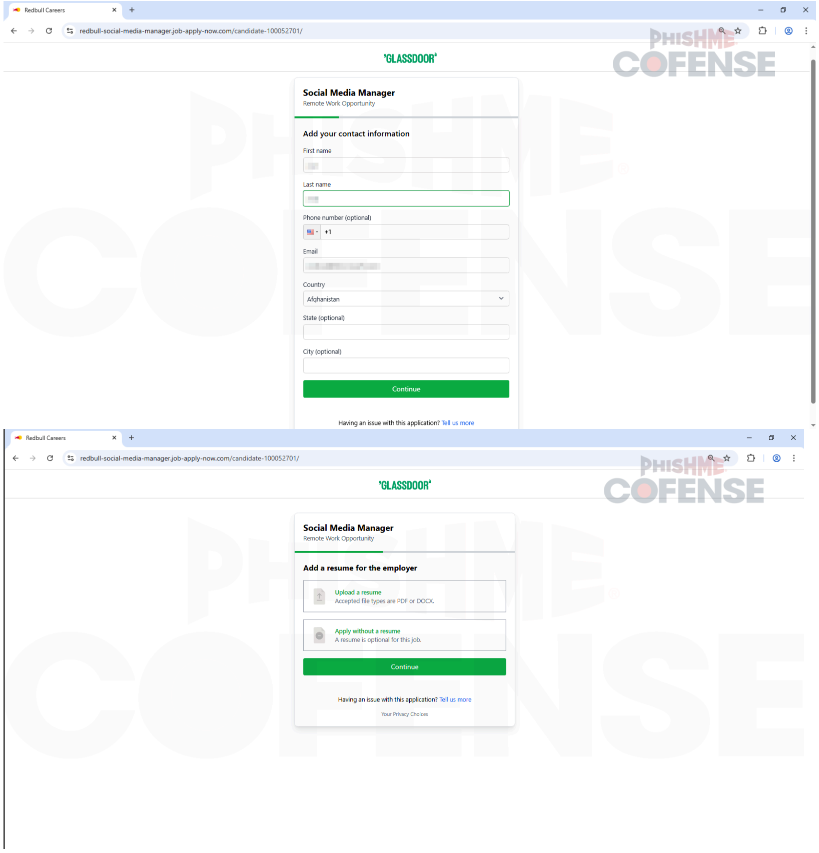
The password that you just used was found in a data breach. Google Password Manager recommends changing your password now.

Job Openings at Google | Goo
Sign in with Google
Sign in with Apple
or
Phone, email, or username
Next
Forgot password?
Don't have an account? Sign up
Elements
Console
Sources
Network
Preserve log
Disable cache
No throttling
Filter
Invert
More filters
All
Fetch/XHR
Doc
CSS
JS
Font
Img
Media
Manifest
Socket
Wasm
Other
Name
X-Login
X-Login
Headers
Preview
Response
Initiator
General
Raw
2 requests
524 B transferred
AI assistance
What's new
What's new in DevTools 137
See all new features
See the highlights from Chrome 137
Facebook - log in or sign up
Google Lens
PHISHME COFENSE
facebook
Facebook connect a with the p your life.
OK
s incorrect.
Forgotten password?
Create new account
Create a Page for a celebrity, brand or business.
English (UK) Español Français (France) 中文(简体) العربية Português (Brasil) Italiano 한국어 Deutsch हिन्दी 日本語
Sign Up Log In Messenger Facebook Lite Video Meta Pay Meta Store Meta Quest Ray-Ban Meta Meta AI
Instagram Threads Voting Information Centre Privacy Policy Consumer Health Privacy Privacy Centre About Create ad
Create Page Developers Careers Cookies AdChoices Terms Help Contact uploading and non-users Settings
Activity log

Figure 8-11: Final Phishing Page for Ferrari

Glassdoor Login Phishing Analysis

This time a new tactic that was utilized by the threat actor, compared to those mentioned in the blog referenced in the Introduction, is the request for the candidate to upload their resume for the Red Bull opportunity. In Job Application Spear Phishing, threat actors were requesting the candidate's Personally Identifiable Information (PII) such as full name, phone number, email address, and physical address on the false Glassdoor page. But this new campaign includes the addition of requesting the user's resume, which reinforces the illusion of this being a legitimate job opportunity, as shown in Figures 12-13. The resume also allows for the threat actor to collect additional PII from the victim that can be used for further social engineering tactics.



Redbull Careers

redbull-social-media-manager.job-apply-now.com/candidate-100052701/

'GLASSDOOR'

Social Media Manager
Remote Work Opportunity

Add your contact information

First name: [redacted]

Last name: [redacted]

Phone number (optional): +1

Email: [redacted]

Country: Afghanistan

State (optional)

City (optional)

Having an issue with this application? Tell us more

Redbull Careers

redbull-social-media-manager.job-apply-now.com/candidate-100052701/

'GLASSDOOR'

Social Media Manager
Remote Work Opportunity

Add a resume for the employer

Upload a resume
Accepted file types are PDF or DOCX.

Apply without a resume
A resume is optional for this job.

Having an issue with this application? Tell us more

Your Privacy Choices

Figure 12-13: Additional

Conclusion

These career-themed phishing campaigns demonstrate how cybercriminals exploit job seekers' trust by mimicking legitimate recruitment practices. By carefully crafting the emails through deceptive login prompts with legitimate logos and brands, as well as the use of multi-step processes, the threat actor creates an illusion of credibility for their campaign. With Cofense's Managed Phishing Detection and Response, we are uniquely positioned to catch phish that have turned up in environments protected by SEGs using human intelligence, advanced technology, and real-time training.

Stage 1 - Observed Email Infection URL:	Infection URL IP(s):
hXXps://www[.]redbull[.]com@rebrand[.]ly/redbull-interview-booking hXXps://study-socialmedia[.]com/workspace/apply hXXps://www[.]career-tesla[.]com/#apply hXXps://rebrand[.]ly/ferrari-recruits	76[.]76[.]21[.]93 66[.]33[.]60[.]35 3[.]33[.]143[.]57 15[.]197[.]137[.]111

Stage 2 - Observed Payload URL(s):	Payload IP(s):
hXXps://redbull-social-media-manager[.]job-apply-now[.]com/candidate-100052701	38[.]114[.]120[.]167 216[.]24[.]57[.]252

hXXps://redbull-social-media-manager[.]job-apply-now[.]com/login_job	216[.]24[.]57[.]4
hXXps://globe[.]anotherlevel[.]app/api/set_status/	146[.]70[.]81[.]214
hXXps://bck-2qw8[.]onrender[.]com/api/create/user	64[.]29[.]17[.]1
hXXps://careers-ferrari[.]com/	64[.]29[.]17[.]65

All third-party trademarks referenced by Cofense, whether in logo form, name form, or product form, or otherwise, remain the property of their respective holders, and use of these trademarks in no way indicates any relationship between Cofense and the holders of the trademarks. Any observations contained in this blog regarding circumvention of endpoint protections are based on observations at a point in time, based on a specific set of system configurations. Subsequent updates or different configurations may be effective at stopping these or similar threats. Past performance is not indicative of future results.

The Cofense® and PhishMe® names and logos, as well as any other Cofense product or service names or logos displayed on this blog are registered trademarks or trademarks of Cofense Inc.