SERVICE ALERT

Prepared Nov 27, 2026, 5:27 PM PST

Be Ware and Be Careful - Impersonate Brands

Status: Ongoing

Started Oct 12, 2026, 10:00 PM PDT

WHAT HAPPENED

A phishing campaign posing as well-known brands, including Google, Nvidia and Coca-Cola, offers paid interviews or webinars to steal work Google and Okta logins. Do not sign in or approve a code or push for any unsolicited invitation, and report it to BIS. We will send more when Google, Okta or the researchers publish new findings.

DOES THIS AFFECT YOU?

Staff who use work Google or Okta accounts can be targeted by fake paid-interview or webinar invitations. If BIS manages your accounts, we are checking sign-in activity for you.

WHAT BIS IS DOING

We are watching the researchers, Google and Okta for new findings on this campaign. We will send the next update when a vendor or researcher reports a change.

WHAT YOU NEED TO DO

Do not sign in to or approve any unexpected interview, webinar or sign-in request, and report it to us. Nothing else is needed for now.

IS THIS A HACK?

Yes — the vendor or a reliable source has confirmed an attack or active exploitation.

LATEST UPDATES

Nov 27, 2026, 5:27 PM PST

Minor new detail: Push Security's teardown gives dates for the American Express and Coca-Cola brand pages and names the first Oct 13 landing page. Still no Google or Okta statement and no fix.

Nov 27, 2026, 5:07 PM PST

New: Push Security's teardown lists block-list domains for the related Google Ads lure, and one summary conflicts with Push on whether it's the same operator; still no Google or Okta statement and no fix.

Nov 27, 2026, 9:03 AM PST

New: researchers link a possibly related Coca-Cola-themed Evilginx campaign that targets Google Ads accounts (link unconfirmed), and the brand list is wider than the page names.

WHAT THE IT COMMUNITY IS SAYING

The only community post I found is an X share of the BleepingComputer article about the GoodGuys fake paid-interview campaign, posted about a day ago (date inferred from the '1 day ago' label). Reddit, Hacker News and IT forums returned no posts from the last 7 days about these lures, the listed landing domains, admin impact, workarounds, or vendor replies.

From public posts by IT administrators; not confirmed by the vendor.

For technical details (versions, patches and sources), ask BIS for the Technical brief.

Questions? Contact BIS Computer Solutions, Inc.

Phone: +1-818-248-5023 · Fax: +1-818-249-1169 · Email: support@biscomputer.com · Web: www.biscomputer.com