SERVICE ALERT

Prepared Nov 27, 2026, 5:27 PM PST

Be Ware and Be Careful - Impersonate Brands

Status: Ongoing

Started Oct 12, 2026, 5:00 PM PDT

WHAT HAPPENED

A phishing campaign is posing as well-known brands and offering paid interviews or webinars to steal work Google and Okta logins. Do not sign in through links in unsolicited invitations, and tell us if you received one. We will send another update if the situation changes.

DOES THIS AFFECT YOU?

Staff with work Google or Okta accounts may receive fake paid-interview or webinar invitations. If you were sent one and signed in, tell us so we can check your account.

WHAT BIS IS DOING

We are warning staff about fake paid-interview and webinar invitations and checking sign-in activity on the work accounts we manage. We will send the next update when a vendor or the research team reports a change.

WHAT YOU NEED TO DO

Do not sign in through links in unexpected paid-interview, webinar or event invitations. Tell BIS if you entered a work password or approved a sign-in prompt.

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

New GoodGuys details (Push Security disclosure, eight impersonated brands, Okta kit support) and a related Microsoft/Google device-code event-invite campaign; no vendor patch or statement exists because this is a phishing campaign, not a software flaw.

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.

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