Hackers Try to Phish United Nations Staffers With Fake Login Pages

By Michael Kan

Published: 2019-10-24 · Archived: 2026-04-05 23:44:59 UTC

Hackers have been creating fake login pages for United Nations websites in an effort to steal the passwords of officials at the UN and its humanitarian groups.

Some of the malicious pages remain live today, according to the security firm Lookout, which spotted the phishing campaign. The pages masquerade as login portals for the United Nations, the UN World Food Programme, and the United Nations Children's Fund (UNICEF), among others. But they are fake pages designed to record whatever the user types into the login fields and send that information to hacker-controlled servers. The "sign in" button does not even have to be clicked; keylogging occurs the moment the user begins typing into the login field.

The sites also adjust based on whether they're accessed on PCs or smartphones. "Specifically, Javascript code logic on the phishing pages detects if the page is being loaded on a mobile device and delivers mobile-specific content in that case," Lookout researcher Jeremy Richards wrote in the company's report. "Mobile web browsers also unintentionally help obfuscate phishing URLs by truncating them, making it harder for the victims to discover the deception."

Lending the fake login pages more credibility is how they can use valid SSL certificates. As a result, the browser will show a padlock button in the web address bar when the malicious login page loads up. Although some of the

past SSL certificates have expired, Lookout uncovered six fake login pages from the hackers that still run valid certificates. (The full site of discovered phishing pages can be found in Lookout's report.)

How the hackers were delivering the fake login pages to potential targets remains unknown at this point. But Lookout speculates it was likely through messages sent via social media, email, or SMS text.

The internet infrastructure behind the fake login pages has been live since March. Other fake login pages masqueraded as login portals for Washington DC-based Heritage Foundation think tank, the University of California, San Diego, along with the German websites for Yahoo and AOL.

Lookout uncovered the phishing campaign through its "Phishing AI," which continuously scans the internet for suspected malicious websites. The security firm has reported the phishing pages to the UN and the law enforcement. So far, the United Nations hasn't commented on the report and whether it's suffered any breaches tied to the phishing campaign.

The fake login pages are a reminder to be careful around your inbox and chat messages. A favored tactic of hackers is sending a message claiming to come from a major internet company, such as Google, Facebook or Netflix, about how there's something wrong with their online account. The email will then contain a link to a fake login page that'll record the victim's keystrokes. So to stay safe, it's good idea to check the web address on any login page to make sure you're visiting the official domain. For more, check out our tips to avoid phishing scams.
