A new WhatsApp phishing site goes live every 2 hours

Last week Meta announced new safety features to protect WhatsApp's 2 billion users from fraud - the features will screen chats for common scam tactics.

Another WhatsApp threat worth knowing about? Phishing domains.

A new study by CNC Intelligence, a digital forensics firm, found 1,216 malicious domains impersonating WhatsApp were registered over a 3-month period. That's 13 being registered every day.

The report tracked every newly registered domain containing "whatsapp" or common misspellings - known as typosquats - then scanned them against multiple independent security engines to confirm malicious activity.

Key findings:

From Dec 10 2025 - March 10 2026, 1,216 malicious domains impersonating WhatsApp were flagged.
1,079 were flagged as confirmed phishing, while 137 were flagged as very likely phishing.
70% of the domains used the exact brand name 'whatsapp', while 30% used common typosquats like "whatsap".
46% of malicious domains used hyphens to mimic real subpages (think: whatsapp-support, whatsapp-login).

How these scams work: a victim receives a link - by text, email, group chat, or social media post - that looks like a legitimate WhatsApp page.

When they click it, they land on a fake site designed to steal their login credentials or personal information.

Matthew Stern, CEO of CNC Intelligence, explained:

"With AI tools, cybercriminals no longer need a skilled developer to clone a professional-looking site. And the sites don't need to fool you for long - they just need your credentials once. After that, the attacker has what they need and the site has done its job. If the site gets flagged and taken down, cybercriminals can quickly replace the site, enabling the scam to continue."

How to spot a fake WhatsApp site:

Double check any URL before you click. Look for hyphens, extra words, or subtle misspellings like "whatsap".
Never log in via a link. If a message asks you to verify your account or log in, go directly to the official site or app and log in from there.
Treat urgency as a red flag. Phishing sites often pressure you to act fast - if a message feels urgent, slow down.

Check who sent the link. These links arrive via text, email, group chats and social media. Even if it looks like it came from someone you know, verify before clicking.

If you are interested in the story, I can provide the full dataset and methodology.