KnowBe4
Human error. Conquered.

Scam of the Week: Phishing for Instagram Passwords

If you're one of Instagram's one billion account holders, then stay on high alert for the latest phishing scam targeted towards the social media platform's users.

The bad guys start the attack by sending an email claiming that someone has attempted to log in to your account. The email is convincing with its simple message and familiar design–complete with an Instagram logo and icon. The email message includes a "sign in" link and a "secure code" to confirm your identity.

When you click the sign in link, you're brought to a completely fake, but extremely realistic-looking Instagram login page. The web address of the login page is the only noticeable red flag. The web address does not include "instagram.com", and the URL ends with ".CF" instead.

Remember the following to avoid scams like this:

- Whenever you're providing login credentials, be certain you're on the real login page.
- Pay attention to the web address and be sure the proper domain is included in the URL.
- When you get an email from an online service that you use, always log in to your account through your browser to check the validity of the message–not through links in the email.

Stop, Look, and Think. *Don't be fooled.*
The KnowBe4 Security Team
KnowBe4.com