



Scam of the Week: PayPal “Unusual Activity” Phishing Scam

The bad guys are trying to steal your personal and financial information again. Their latest scam is a phishing email that appears to come from your PayPal account.

Here’s how it works:

1. The phishing email claims that an unknown device has accessed your PayPal account, and to protect your account and your money, you have to “verify your identity” by clicking a link and following verification steps.
2. After clicking the link, you’re brought to a webpage that instructs you to complete a CAPTCHA prompt, where you must enter a code and then click a button to continue “securing your account”.
3. Finally, you’re brought to a fake PayPal login page to enter your PayPal login credentials. If you enter your credentials, you’re then instructed to submit personal and financial details, and even the login information for your email account.

If you submit your login credentials or personal information, your PayPal account can now be taken over by the bad guys, and your account and personal data are at risk.

Remember these tips to keep your PayPal account—and other online accounts—safe:

- Never click on links in an email you weren’t expecting.
- When you receive an email asking you to log in to an account or online service that you use, log in to your account through your browser—not through links in the email. This way, you can ensure you’re logging in to the real website.
- Do not reuse passwords. If you use the same password for different accounts and one gets hacked, they all are.

Stop, Look, and Think. Don’t be fooled.

The KnowBe4 Security Team

KnowBe4.com