Scam of the Week: Beware of Amazon Prime Day Phishing Scams

Cybercriminals are famous for impersonating well-known brands or services in order to trick you into falling for their scams. Since you're already receiving numerous emails about it, the bad guys know Amazon's Prime Day is a great opportunity to tempt you with a great "deal".

The bad guys are selling so-called "phishing kits" that make it easy for any aspiring hacker to craft legitimate-looking emails appearing to come from well-known companies. The attackers are using these phishing kits to craft fake emails for Amazon's Prime Day. The emails include a PDF attachment containing a dangerous phishing link. If you click the link, you're brought to a fake Amazon login page and prompted to sign in to claim your Prime Day deals. If you sign in to this bogus page, your Amazon account will be compromised. If you use the same or similar passwords for other accounts, those accounts could also be compromised.

Always remember the following to protect yourself from scams like this:

- Never click on links or download attachments from emails you weren't expecting–even if it appears to be from a legitimate organization.
- When logging in to any online service, never use the link in the email. Always type the web address into the browser yourself or use your normal bookmarks instead.
- Never reuse passwords across multiple sites. Consider using a password manager to keep your login details secure.
- When it comes to Prime Day or any type of "deal"–if something sounds too good to be true, it probably is. Delete suspicious emails or follow the reporting procedures put in place by your organization.

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