SCAM OF THE WEEK:

Advanced Attacks from APT35

A cybercriminal group known as APT35 has been targeting high-profile organizations in government, journalism, higher education, and more. For a more convincing attack, APT35 compromises legitimate websites that work with these high-profile organizations.

Once they've compromised a website, APT35 uses the website to send phishing emails to their targets. For example, in one attack APT35 sent emails with phony invitations to an upcoming webinar. These invitations included a link to the compromised website. If you clicked on the link, you were brought to a registration page. On this page, you would be asked to sign up using your email credentials. APT35 wants you to hand over your credentials so that they can gain access to your account, personal information, and eventually your organization.

Use the tips below to recognize similar advanced attacks:

- When you receive an email, stop and look for red flags. For example, watch out for emails that were sent outside of business hours and emails that contain multiple spelling or grammatical errors.
- Never click a link in an email that you weren't expecting. Even if you recognize the email sender, consider what the link is for and why it was included in the email.
- When in doubt, contact the sender by phone or in person to confirm the legitimacy of the email.

The KnowBe4 Security Team
KnowBe4.com

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