Scam of the Week: Phony LogMeIn Security Updates

LogMeIn is a popular remote access tool used by IT professionals to gain entry to their employees' machines. These tools are especially popular right now with so many people working remotely. Unfortunately, with popularity, comes risk. Cybercriminals are impersonating LogMeIn in a new phishing attack. The phishing email claims that you need to click a link in the email to download an "urgent security update". If you click this link, it takes you to a phony login page for LogMeIn. If you enter your credentials on this look-alike page, the information will be sent straight to the bad guys. If you fall for this trick, you could give attackers access to countless machines within your organization's network.

Stay safe by following these tips:

- Never click on a link within an email that you weren't expecting.
- If you are prompted to update any software on your work device, reach out to your administrator or IT department so they can check that the update is legitimate and safe.
- When an email asks you to log in to an account or online service, log in to your account through your browser–not by clicking the link in the email. That way, you can ensure you're logging into the real website and not a phony look-alike.

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