Image Licensing and Phishing Scam

Website Support · https://missionsupport.archden.org/knowledgebase/image-licensing-and-phishing-scam/

Don't Click That Link!

If you get an email regarding your website and a possible legal action against you, it is very possible that it is a scam. A new scam targeting companies and website owners have been threatening legal action for alleged copyright infringement on their stolen copyrighted images. Instead of identifying the image, the scammer instructs you to click a link where you can supposedly see the image(s) that infringes on their copyright. That link will either lead to a phishing site where you are tricked into handing over information/money, or it downloads malware. If you encounter this message, we strongly recommend that you do not click any links, delete the email, and/or to mark the email or comment as spam.

Signs of a Scam

- **Check the spelling** – an obvious giveaway is bad spelling. Keep an eye out for this, delete or send it to IT to examine.
- **Hover before you click** – Phishers often try to hide their URLS leading to their malware. Hover over hyperlinks before you click, and this will reveal the true URL destination, no matter what the linked text says.
- **Be suspicious of generic greetings** – generic greetings , especially ones regarding finances, are suspicious.
- **Be wary of attachments** – unexpected attachments should not be opened, the risk is not worth it.
- **Do not be intimidated** – phishing emails often try to get an emotional response, especially by using language that is threatening. Other examples include emails claiming to be from a bank or a law enforcement agency, threatening account closure or arrest if immediate action is not taken.

- **There is a time sensitive threat** – phishing requires you to be tricked and to get what they want fast.
- **If the message is in a comment on your site** – there are other more direct ways to contact you. No legitimate threat would be put into a comment.

What if it is real?

If you have used copyrighted images without permission, either get permission of replace them with images that do not require attribution or permission. Removing the offending content should be enough to satisfy the real copyright holder.

If you do not have any copyrighted images or other content on your site that you're using without permission, then you have nothing to worry about and you can ignore the threat. Make sure to delete the message, report it to IT, and/or mark it as spam.

References:

Paul Bischoff, 2021, *Don't Click the Link! Scam threatens website with copyright legal action*, Comparitech, viewed June 24, 2021, <https://www.comparitech.com/blog/information-security/copyright-infringement-scam/>

Wedgewood Team, 2020, *Copyrighted Image Scam*, Wedgewood Insurance, viewed June 24, 2021. <https://wedgwoodinsurance.com/blog/commercial-insurance/copyrighted-image-scam/>