BZMM
BLUEZONE MOBILE MEDIA

Scammers are targeting Facebook users through deceptive messages, falsely claiming that their Facebook page has violated copyright issues or that there is something on your account that needs urgent attention and intervention. This issue seems to be getting worse daily and especially over festive and holiday seasons. They particularly target accounts that are running paid adverts as they know that these accounts are very active. I want to emphasize the importance of NOT clicking on any links within these messages and refraining from responding to them.

These messages are phishing attempts designed to trick unsuspecting users into providing their sensitive information, such as passwords, with the intention of compromising their Facebook account. It is crucial that you remain vigilant and take the necessary precautions to protect your Facebook page and personal data. Whilst these messages may seem convincing at first glance, if you look closely, the spelling in their message is atrocious and the names & icons look ridiculous to the trained eye.
The official Facebook teams would never send these messages in this manner.

Instead of clicking on any suspicious links or engaging with these spam messages, I strongly advise you to follow these very important steps to ensure the security of your Facebook page if you have concerns:

1. Do not click: Avoid clicking on any links within messages that claim your Facebook page has violated copyright issues. These links are designed to deceive you and could lead to unauthorized access to your account.

2. Ignore and delete: If you receive such messages, treat them as spam and delete them immediately. Do not respond or provide any personal information.

3. Check page health via settings: To monitor the status and health of your Facebook page, access your Facebook account and navigate to the settings tab specifically dedicated to your page. This will allow you to review any warnings or notifications directly from the official Facebook platform.

4. Enable two-factor authentication: Activate two-factor authentication for your Facebook account to add an extra layer of security. This will require a second form of verification, such as a code sent to your mobile device, when logging in.

5. Educate your team: Ensure that all staff / individuals who have access to your Facebook page are aware of these phishing attempts and understand the importance of avoiding suspicious links and messages. By following these precautions, you can significantly reduce the risk of falling victim to phishing scams and protect your Facebook page from unauthorized access.

Thank you for your attention to this matter, and please remember to remain cautious while using social media platforms. Together, we can stay one step ahead of scammers and protect our digital assets.