DATCP: Consumer alert: Facebook-related phishing scams

Posted on Thursday, Sep 1, 2022

MADISON, Wis. – A large number of fraudulent messages claiming to be Facebook customer service representatives or automated customer service systems have recently been reported to the Wisconsin Department of Agriculture Trade and Consumer Protection's (DATCP) Bureau of Consumer Protection. These messages claim that a recipient's Facebook account has been hacked, stolen, or disabled, and urge them to click a link in order to recover their account. If the link is opened, users are asked to "log in" to a website that appears very similar to Facebook but is actually a convincing fake set up by scammers to steal account information.

This practice is known as a phishing scam and may target specific individuals or thousands of people at once. The recent Facebook-related phishing attempts usually arrive via email, text, or Facebook private messages. Similar phishing scams may occur through Facebook Marketplace, Facebook Groups, a friend's hijacked Facebook account, Instagram, or WhatsApp. If you receive an unsolicited message about your Facebook or other social media account being compromised:

- Do not reply to the message, call, or text any number provided in the message.
- Do not provide any of your account information or passwords.
- Do not click any links or open any attachments in the message. These may contain viruses or malware that could be installed onto your device without your permission or knowledge.
- If you do click on a link in a suspicious message, you may want to have your device scanned for viruses and malware at a reputable computer or cell phone repair establishment. Change your passwords on a separate, secure device as soon as possible.

Users should not panic or feel intimidated if they receive these messages about compromised accounts as Facebook will never contact users via text or private message. If users are unsure of an email's legitimacy, they should check the sender's address to make sure it's an official Facebook account. They can also hover over links in the email message without clicking or opening them to see the web address to which they lead. Facebook users concerned that their account may be compromised can seek help at facebook.com/hacked. Although Facebook is the most commonly impersonated social media platform by phishing attempts due to the social media platform's popularity, it is not the only one that scammers utilize.

For additional information and consumer protection resources or to file a complaint, visit the DATCP's Consumer Protection webpage at ConsumerProtection.wi.gov. If you have questions or believe you are a victim of a scam, report it by calling DATCP's Consumer Protection Hotline at 1-800-422-7128 or emailing DATCPHotline@wi.gov.