PHISHING AND EXTORTION SCAMS AFTER SECURITY BREACHES

Consumer Alert

In the news:

A recent attack on Facebook's computer network exposed the sensitive personal data of millions of users. That information could be used in phishing and extortion scams.

What you need to know

Phishing is a type of scam that starts with an email, text message, or phone call that pretends to be from a legitimate source. The message will tell a plausible story related to a need for you to verify or provide your personal information. The goal is to get you to enter your personal information into a fake website or extort money from you.

Phishing scammers try to get their hooks in you. Don't take the bait. Learn the signs of a phishing scam and the steps you can take to avoid being scammed. Read our Consumer Alerts Fraudulent E-Mail Thieves Intend to Steal Your Personal Information and Data Breaches: What to Do Next.

Remember

These scams may use recently hacked data as well as data hacked years ago.

Recent extortion phishing scam

The Attorney General has received reports of a recent scam using hacked information threatening to expose the recipient's alleged viewing of adult videos unless the sender is paid $1,000 in Bitcoin. The email was fraught with misspelled words, grammar errors, and mismatched links. However, the email correctly cited the recipient's password information for an online account.

SPOT IT: Watch out for phishing attempts.

- Look for messages with misspellings, typos, and bad grammar.
- Look for messages that use your password or some of your personal information.
- Look for mismatched links that you can spot by hovering your mouse over a link that does not match the stated destination.
- Beware any unsolicited message that asks you to click on a link, open an attachment, or verify your personal information.

STOP IT: Consider what you share and who you share your personal information with.

- Never reply to emails, calls, texts, or pop-ups that ask for verification or your personal information.
- Review your privacy settings and take advantage of Facebook's security options.
- Change your passwords and security questions: do not recycle old passwords.
- Report suspicious emails and Facebook messages to phish@fb.com.

To report a scam, file a complaint, or get additional information, contact the Michigan Department of Attorney General:

Consumer Protection Division
P.O. Box 30213
Lansing, MI 48909
517-335-7599
Fax: 517-241-3771
Toll free: 877-765-8388
Online complaint form

Dana Nessel
Attorney General