Avoiding PHISHING SCAMS

Phishing attempts can be very sophisticated, often appearing as legitimate communications from trusted sources. Protect yourself by being vigilant with these simple tips.

Recognize the Signs

- Generic greeting like "Dear Customer"
- Requests for personal or financial information
- Suspicious links or attachments
- Calling for urgent action
- Email address that doesn't match the supposed sender
- Spelling or grammar mistakes

Resist and Report

Resist replying, clicking on links, downloading attachments, or taking action presented in message.

Report the suspicious message by using the "report spam" feature and alert trusted organizations that message may have resembled.

Delete the Message

Again, don't click on any links, including "unsubscribe links" as they could be potential phishing attempts as well.

Delete the message!
DELETE. DELETE. DELETE.

And repeat this for any other suspicious messages.

Banking ALERT: Your account has been locked

B fraudunit@bankofamirica.com
To Bradley Cooper, DDS

Hello Online Banking Customer,

Several login attempts have been made on you're account. As a result, we have temporarily locked your account. For added security the fraud unit has added an extra verification process.

To begin the verification process, please click here. If you fail to update your account information within the next 48 hours, your account will have to be manually unlocked by visiting a local branch.

Sincerely,

Bank of Amirica Fraud Detection
fraudunit@bankofamericas.com
888-555-1234

Phishing Email Example