How to Spot **SCAMS**

Heartland CREDIT UNION

EMAIL PHISHING SCAMS

Do you know how to spot them? This example and the tips below will help you recognize a suspicious email.

Email

Inbox (9)
Sent
Drafts
Spam
Trash

ACTION required or your account will be DELETED 1

Joe Shabadoo <jshabadoo@grnail.com> 2 Jan 26 at 3:29 AM 3

Valued Customer, 4

Someone has gained unauthorized access to your account. Reset your Pass Word imediately. 5

RESET PASSWORD 6

Customer Support: http://youraccount.com/dcijflksd%al
Questions? Contact: 1-800-555-3942 7

View Attachment: Status_Report.doc.file 8

KEEP AN EYE OUT FOR THESE RED FLAGS

1. **The subject line** Scammers tend to use an urgent or aggressive tone.
2. **The sender** In the example above, is the sender using a Gmail address? If you said yes, take a closer look! It's actually g-r-n-a-i-l.com. Sneaky scammers will use email handles that are one letter off from what they should be (e.g., "netftix" instead of "netflix") so that, at a glance, everything appears official.
3. **The time stamp** When was the email sent? This is an especially telling clue when a scammer is impersonating someone you know or correspond with regularly.
4. **The greeting** Does it address you by name, by email address or by a generic title? A generic or awkwardly phrased greeting could be the sign of a scam.
5. **The spelling** Errors in spelling and grammar are always a red flag.
6. **Buttons and links** These are easy for scammers to format and disguise. Get in the habit of accessing your accounts by typing the official URL in a new browser window. Avoid using the direct links in your email messages.
7. **The contact info** Does it look sketchy? If you need to verify the legitimacy of the sender, never use the contact information contained within the email. Cross-reference it with a separate web search.
8. **Attachments** Malicious files can be easily disguised as innocent Word documents, spreadsheets and presentations. Be deliberate about which attachments you choose to open or download.

REPORTING EMAIL SCAMS

Email phishing attempts (even the unsuccessful ones) can be reported here:

Internet Crime Complaint Center (IC3)
www.ic3.gov

Federal Trade Commission (FTC)
www.FTC.gov/complaint