Cyber scam spotter
Signs of scams

As the public is catching on to phishing emails and cybercrime, scammers are working hard to figure out new ways to steal identities, account information and money. Yet, despite the increased awareness, many phishing emails are still written using the same scam tactics.

Keep an eye out for these clues so you don't get caught in a phishing scam.

1. **If you don't recognize the sender, don't open the email.**
2. **Extreme or strange subject lines:** Watch out for subject lines that say "Urgent" or that don't make sense.
3. **Generic greeting:** Scam emails are rarely personalized. Instead, they may start with a generic "Hello."
4. **Spelling and grammar:** Fraudulent emails often have misspelled words and poor grammar.
5. **Scare tactics and urgent language:** Fraudulent emails often try to scare you into thinking something bad will happen if you don't respond with your account information or other confidential information. For example, you may get an email saying your account is suspended and the only way to make it active is to verify your account information.
6. **Requests for personal information:** U.S. Bank will never ask for confidential information (Social Security number, account numbers, password, name/address) in an email or text message. The bank will only ask for this information when you call its toll-free Customer Service numbers. Rule of thumb: Never provide information you wouldn't write on a postcard.
7. **Links or attached documents in an email:** Beware of any hyperlinks and attachments in emails. Clicking the link or opening the attachment may bring you to a fraudulent site or download malicious software that may lock your computer. Look for sloppy clues in the link. For example, "usbanks" instead of "usbank."

From: (1) sally.smith@habanks.bank
To: Charles Jackson
Subject: (2) URGENT payment overdue

Urgent payment due

(3) Hello,

(4) I writing you to imforn you that your account is 120 days over due and we have not yet recieved paymet for our services.
(5) If we do not receive we will take legal action against you.

To immediately make a payment, please click the link to visit a secure website where you can make a payment.

Once you have made an account at our page, (6) enter your credit card and make a payment.

(7) http://www.habanks.banks

If you spot a suspicious email claiming to be from U.S. Bank, please forward it to fraud_help@usbank.com or call the Fraud Liaison Center: 877.595.6256.

For more information visit **usbank.com/online-security.**