CAN YOU SPOT PHISHING E-MAIL?

E-mail address. Closely monitor email addresses. Make sure they match the company's URL.

From: Smarter Bank Customer Service <customerservice@smartrbank.com>

Attached Download.txt .txt File

Questionable attachment. Never download attachments you aren't expecting.

Subject: **Card Account Access**

Bad graphic. Be leery of fuzzy, pixelated, or mismatched graphics.

Dear Valued Customer ,

Awkward Spacing

Are part of our on-going security, we continuously monitor for suspected logins from unknown locations. Our systems show a suspected login (details below).

Grammatical Errors

gin Details: September 4, 2020, at 2:48pm from Genoa, IL.

If this is correct, your there is no need to respond. If this not, we recommend that you change your password immediately using the link below. You may also find further instructions in the attached document.

Urgency. Slow down to think. Hackers thrive when users make rash decisions.

Update Account Info

Account Information. Never click links claiming to relate to your account info unless you were expecting an e-mail from the person or company.

Unusual Closing

Best of thanks,
Aberjo Thomas
Security Customer Relations
customersupport@smarterbank.com
1711 17th SE - Montreal, KA 40052

http://kazzuu.net/kllIssie8
Click or tap to follow link.

Incorrect URL. Hover over buttons to reveal where the link will lead.

Strange address. Check to see if the physical address is accurate.

If you suspect you have received a phishing e-mail, contact IT immediately.

Pratum
pratum.com