Don't Fall for Fraud

EMAIL SCAMS

Check out this FRAUDULENT email below:

URGENT: Account activity alert

info@pinecreek-bank-us.co **1**

Dear Customer

We received a mobile request from you, or someone with access to your account, to make changes to your Pine Creek Online Bank Profile.

If you did not authoize thes changges, please varify your account with your **2** account PIN or Social Security Number through the link below!
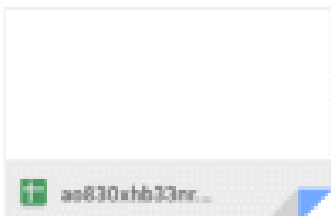
Sign On below to verify you account dettails. Note that entering incorrect account information will result in your account being closed IMMEDIATELY! ACT NOW! **3**

Verify your Pin or SSN

https://www.pinecreek-bank-us.co/log-in **4**

or view your account transactions attached

ae830xhb33nr... **5**

Let's Take a Closer Look

#1 Unusual Email Address

Slow it down. Does that look like an email address your bank would use? Be wary of unexpected emails from addresses that aren't like the ones your bank typically employs?

URGENT: Account activity alert

info@pinecreek-bank-us.co **1**

#2 Misspelled Words

Spot check! If you see misspelled words or odd grammar, they are all clear signs of an impersonator. *Real banks use spell check.*

Dear Customer

We received a mobile request from you, or someone with access to your account, to make changes to your Pine Creek Online Bank Profile.

If you did not authoize thes changges, please varify your account with your account PIN or Social Security Number through the link below! **2**

Sign On below to verify you account dettails. Note that entering incorrect account information will result in your account being closed IMMEDIATELY!

#3 Scare Tactics

Don't panic. If an email uses scare tactics, such as urgent warnings of account closure or security breaches, you can safely assume it's a scam.

Sign On below to verify you account dettails. Note that entering incorrect account information will result in your account being closed IMMEDIATELY!
ACT NOW! **3**

Verify your Pin or SSN

#4 Suspicious URLs

Banks will never ask you to log in via email. Phishing emails use deceptive URLs to take you to malicious websites. Never click links that you weren't expecting.

https://www.pinecreek-bank-us.co/log-in **4**

or view your account transactions attached

#5 Unexpected Attachments

Something's "phishy," because real banks will never send an email attachment — especially when you didn't ask for it. Attachments can contain malware that can compromise your computer or personal information. Never click on attachments from emails supposedly from your bank.

5

as830xhb33rr...