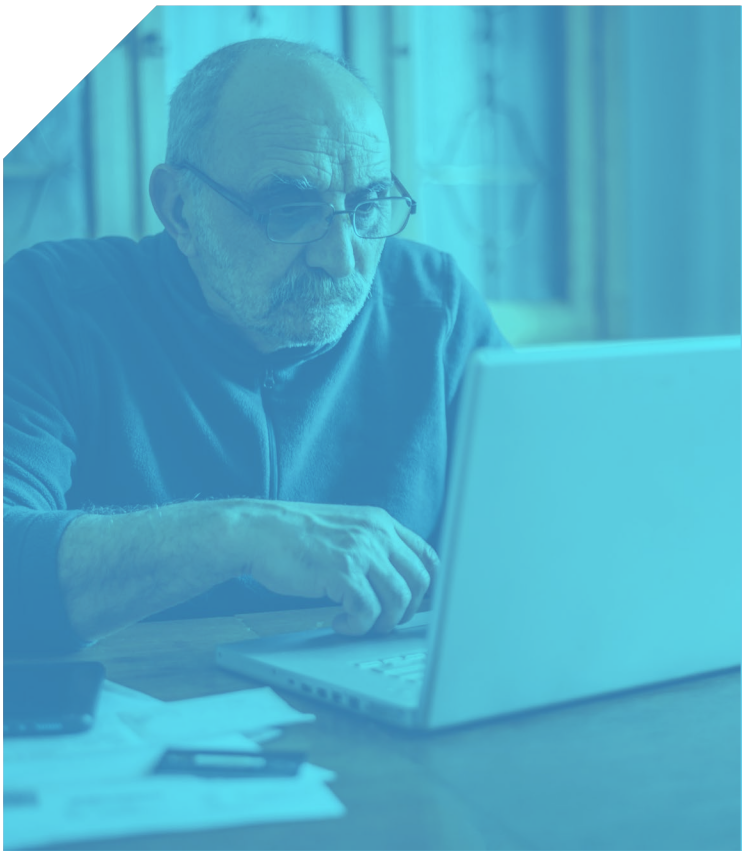


Capitol Federal®

When Good People Fall Victim to Bad Scams

And the Tools We Need to Stop Them

At Capitol Federal®, your security is our priority

Financial scammers are extremely skilled at what they do. Each year, they grow more sophisticated, more cunning, and more deceptive. Good people, just like you, become victims of their crimes every day. Fraudsters frequently rely on fake emails, texts, and phone calls that can look and sound convincingly real.

At Capitol Federal®, we're dedicated to helping you protect your identity and resources. Scammers use many of the same tactics across texts, calls, and emails. The contact is usually unexpected and may be designed to create a sense of fear or concern for someone you care about. They may urge you to act immediately. With a few simple, consistent habits, you can spot a scam and keep yourself safe.

No matter how much we work behind the scenes to protect your information, the most powerful defense starts with you and can be summed up in three words:

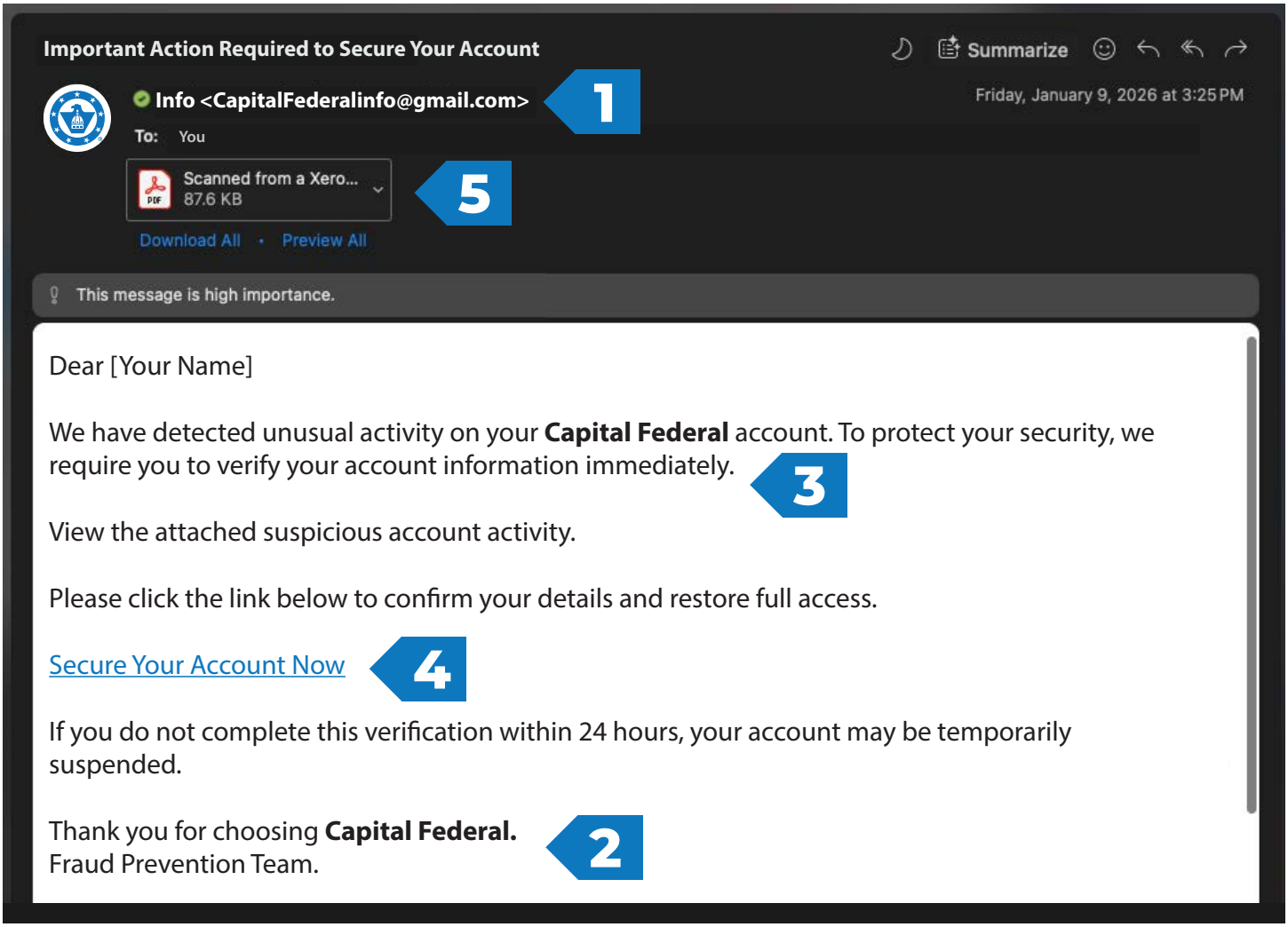
Pause. Reflect. Protect.

Pause.
Take a moment to step back from the call, text or situation. Be intentional about pausing your involvement.

Reflect.
Consider the reasonableness of the call, text, or situation. Does the scenario seem plausible? Is there a sense of urgency or emotional pressure?

Protect.
Take action to ensure safety by ending the communication. Contact the bank or company on their published phone line to confirm. Use strong passwords and security software to prevent hacking.

How to Spot Email Scams



1. Unusual Email Address
Does it look like an email address your bank would use?

2. Misspelled Words
Misspelled names, words and odd grammar are all signs of a scam.

3. Scare Tactics or Pressure
If an email uses scare tactics or urgent warnings, it is safe to assume it's a scam.

4. Suspicious URLs.
Banks will never ask you to log in via an email. Never click the links.

5. Unexpected Attachments
Real banks will never send you an attachment – especially when you didn't ask for it.

How to Avoid Phone Call Scams

Unusual Caller ID

Do NOT rely on caller ID, it can be spoofed. If you receive an unsolicited call purporting to be your bank, be very skeptical.

Scare Tactics or Threats

If the caller pressures you for immediate action or threatens negative consequences, just hang up and call your bank directly.

Asking for Personal Information

Never share confidential details unless you've called the number for your bank.

Unexpected Call

Not sure? Stay safe by ending the call and dialing the number on your bank's website or the back of your bank card.

How to Spot a Text Scam

Strange Phone Numbers

Slow down! Legit text messages come from an official 4 to 5-digit number.

Urgent Warnings or Requests

Real banks won't text threatened actions or urge you to log in immediately.

Odd Grammar or Spelling Mistakes

Spot check. Real banks use spell check.

Request for Personal Information

You will NEVER be asked to provide personal information in a text. It's a scam.

Suspicious Links

DON'T click the link. Instead, visit your bank's official website or call the published number for your bank.

For more tips and tools to help you stay protected, visit our website at the secure address: www.capfed.com/fraud

Also, call us at 1-888-8CAPFED to report any unusual activity related to your accounts.

If you believe you have been victimized as a result of a scam or identity theft, report the event to your local law enforcement. You can also report identity theft to the Federal Trade Commission online at www.identitytheft.gov.
Online scams can also be reported to the Federal Bureau of Investigation's Internet Crime Complaint Center at www.IC3.gov.