

How to Spot Phishing Scams Before It's Too Late

Think before you click.

Cybercriminals are getting better at making fake emails look legitimate. They mimic banks, nonprofits, government agencies, coworkers, even organizations you trust. Often, they create urgency and pressure you to click before you have time to think. The good news: most phishing scams follow predictable patterns.

1. Be Suspicious of "Secure Message" Emails

One of the most common phishing tactics is a message that says:

- You have received a secure email
- Click here to view an encrypted message
- Open message to see an important notice
- Your account has been suspended

These messages often include a big button like "Open Message." That alone doesn't make it fraudulent—but it should make you pause.

Red Flags:

- You weren't expecting a secure message.
- The sender's email doesn't match the organization.
- The message contains little or no actual content.
- It pushes you to click a button rather than replying normally.
- It uses urgency or vague warnings.

2. Check the Sender's Real Email Address

Don't just look at the display name.
Scammers fake names.

A message may say it's from:
American Legion Department of California

But the actual sender could be:
nonnym@staffvision.co.za

That's a major red flag.

Ask:

- Does the domain match the organization?
- Does it come from an unexpected country domain ([.co.za](#), .ru, .cn)?
- Is it slightly misspelled?
 - [paypal.com](#) (capital "l" instead of lowercase "l")
 - [micros0ft.com](#) (zero instead of "o")

3. Hover Before You Click

Before clicking any button:
Hover over the link (don't click).

Check where it actually goes. Usually when you hover, you can see the link at the bottom left of your browser on a desktop or laptop.

If "Open Message" points to:

- a random Microsoft login page
- a shortened link ([bit.ly](#), tinyurl)
- a domain unrelated to the sender
- a misspelled or suspicious URL

...don't click.

4. Watch for Emotional Pressure

Phishing often uses fear, urgency, or authority.

Examples:

- Your account will be suspended.
- Immediate action required.
- Confidential legal notice.
- Payroll issue.
- Security alert.
- Committee appointment suspended.

Scammers want panic to override judgment.

5. Be Wary of Login Requests

A classic phishing trick:

1. Fake email
2. Fake "secure message" portal
3. Fake login screen
4. Stolen password

If clicking an email takes you to a login page asking for credentials:

Stop.

Go to the organization's real website manually instead.

6. Verify Through Another Channel

If something seems off:

- Call the sender.
- Start a new email thread.
- Text the person.

- Log into the organization's portal directly.

Never verify by replying to the suspicious email itself.

7. Look for Generic or Odd Formatting

Common clues:

- Strange spacing
- Awkward wording
- Low-quality logos
- Broken formatting
- Generic greetings ("Dear User")
- Buttons with vague text ("Open Message")

Sometimes the email looks polished.

Sometimes the scam is hiding in the details.

8. Trust Your Instincts

If you find yourself thinking:

- "This feels weird."
- "Why would they send this like this?"
- "Why is this coming from South Africa?"
- "Why can't they just email me normally?"

That instinct is worth listening to.

If You Think You Clicked a Phishing Link

Act quickly:

1. Change your password immediately.
2. Enable two-factor authentication.
3. Notify your IT department or email provider.
4. Scan your device for malware.
5. Monitor financial and online accounts.

Fast action can limit damage.

A Simple Rule

Don't trust the email. Verify the sender.
That one habit prevents most phishing attacks.

Final Thought

Phishing isn't always obvious anymore.

Some scams look professional. Some imitate real organizations. Some use legitimate-looking "secure message" systems to steal credentials.

But most still reveal themselves if you slow down and inspect:

- Who sent it
- Where the link goes
- Why it feels urgent
- Whether the request makes sense

Pause. Verify. Then click.

That pause may save your accounts—and your identity.