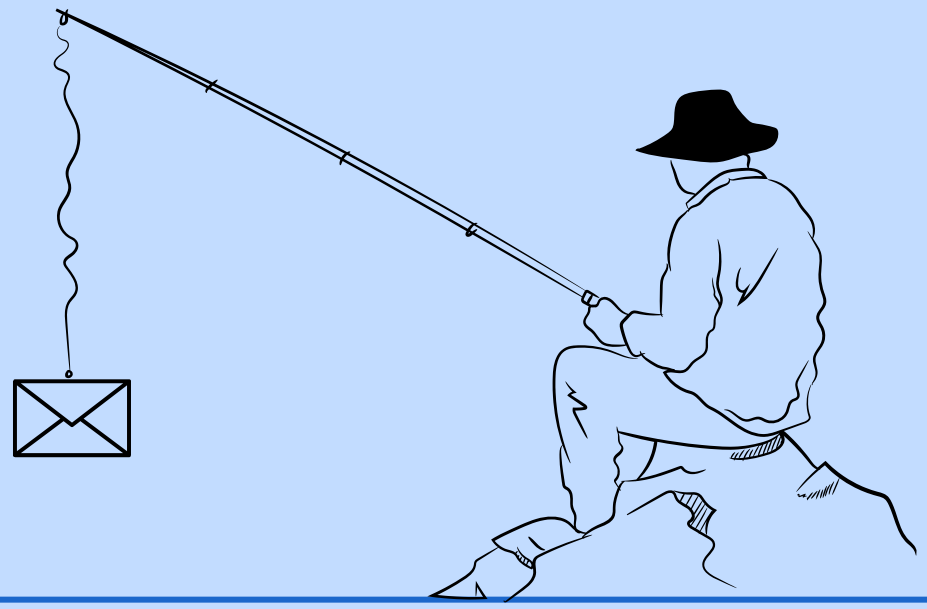
@SBTPARTNERS

The Anatomy of a Phishing Email

HOW SMBS GET TRICKED—AND HOW TO STOP IT.



Swipe →

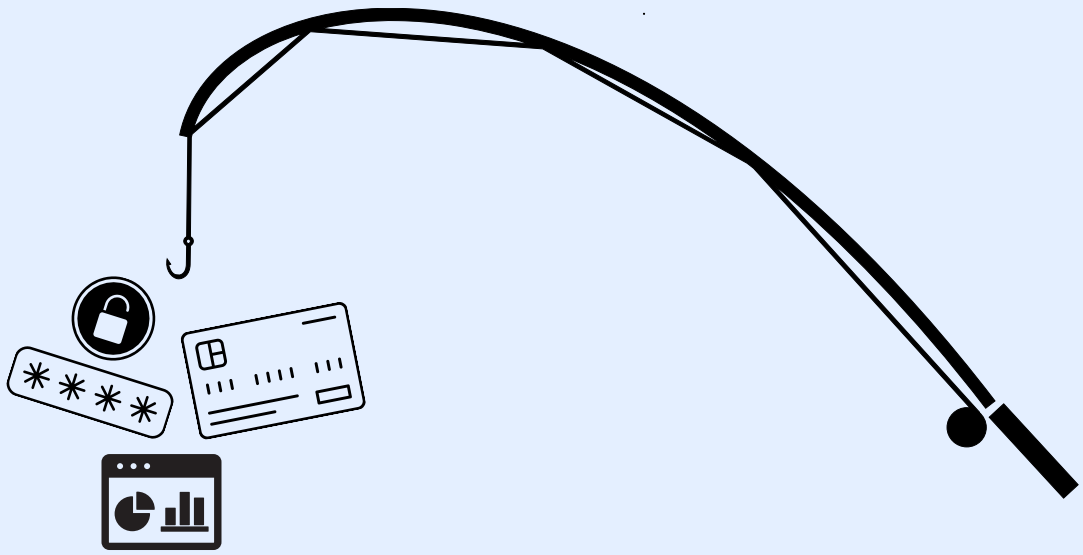
SBT PARTNERS

What is phishing?

Phishing is a type of cyberattack where criminals impersonate trusted sources—like banks, coworkers, or vendors—to trick you into giving up sensitive information. These attacks often come in the form of emails, texts, or fake websites designed to look legitimate.

What Are They After?

- Passwords
- Credit card numbers
- Company data
- Access to your network



Swipe

@SBTPARTNERS

What Phishing Looks Like

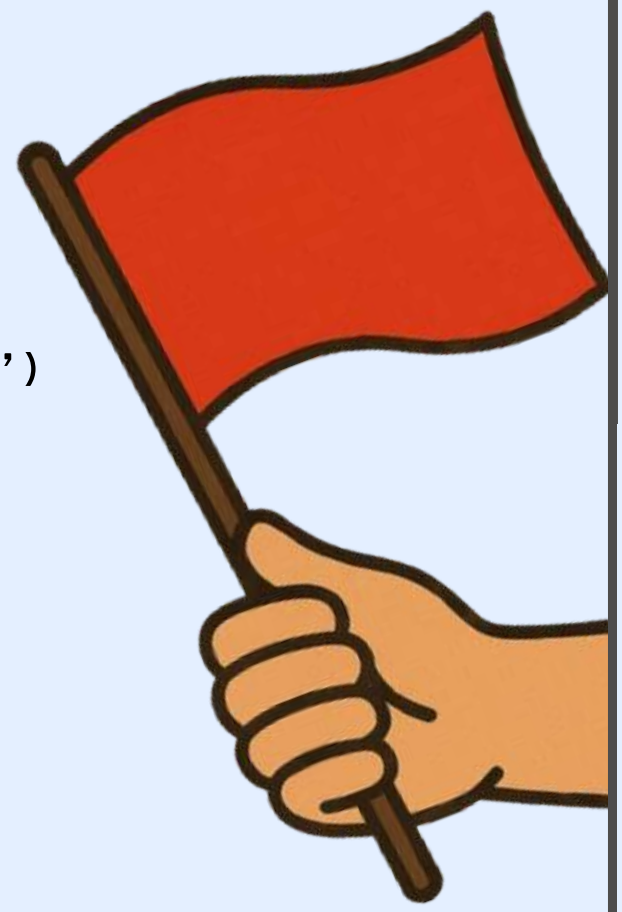
- A message that looks legit: from a bank, vendor, or even your boss.

- Urgent tone: “Act now!” or “Your account is compromised.”

- Suspicious links or attachments.

Swipe

Red Flags to Spot



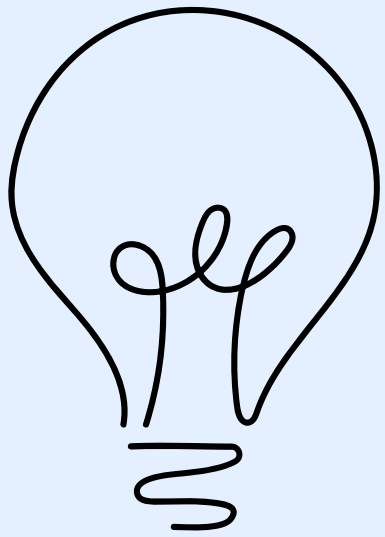
- Misspelled domains (e.g., microsOft.com)
- Generic greetings (“Dear user”)
- Unexpected attachments
- When you Hover-over links, It doesn’t match the sender

Swipe →

@SBTPARTNERS

Prevention Tips

- Hover over links before clicking—check the actual URL.
- Don’t open unexpected attachments.
- Verify requests by calling the sender directly.
- Use multi-factor authentication (MFA).
- Keep software and antivirus up to date.

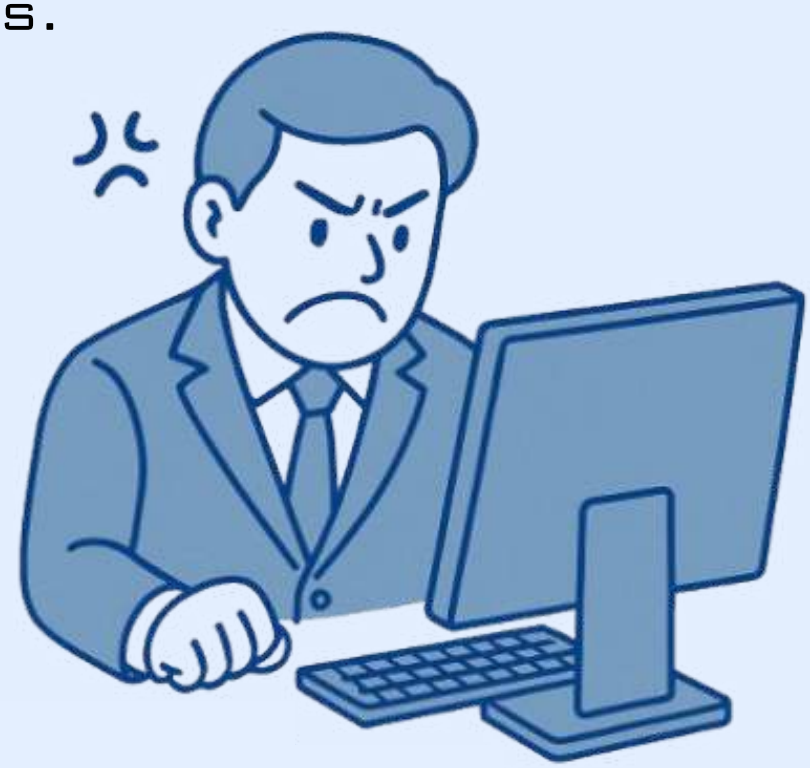


Swipe

@SBTPARTNERS

Real-World Example

- An employee clicked a fake invoice from a vendor.
    - Malware is installed.
        - Company loses access to files for 3 days.

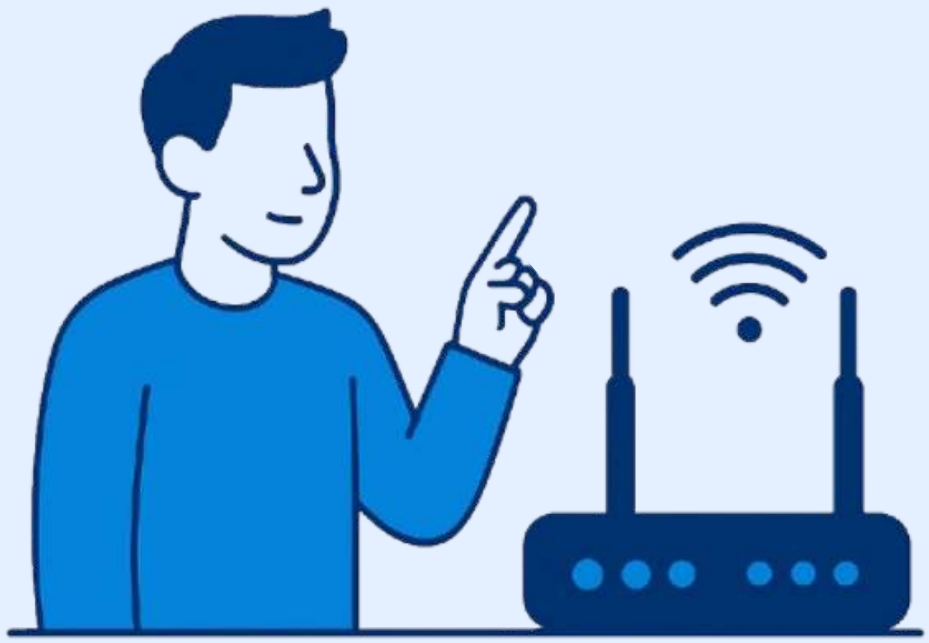


Swipe →

@SBTPARTNERS

What to Do If You Click

- Disconnect from the network immediately.
- Notify your IT team or provider.
- Don’t try to fix it yourself.
- Change passwords and monitor accounts.



Swipe →

@SBTPARTNERS

@SBTPARTNERS

Get Phishing Training with SBT

DON'T LET ONE CLICK COST YOU THOUSANDS.

Upgrade your MSP today at sbtpartners.com

your first line of defense starts here.

THE SBT PARTNERSHIP

SBT PARTNERS