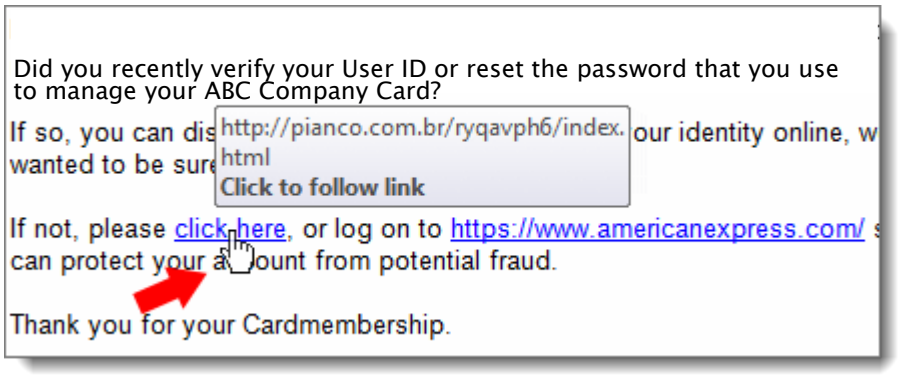
HOW TO IDENTIFY A PHISH

Phishing is the act of sending out a **fake email** that **looks like it's legitimate** to trick you into giving out **personal information**. Some phishing emails contain **malware attachments**.
Your information is then used to gain access to your personal or business accounts to inflict damage (monetary or otherwise.)

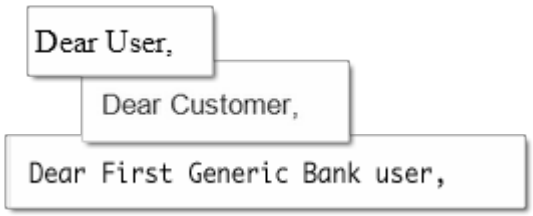
Look through the examples so you know how to spot a phishing attempt.

Hover over links to investigate



Analyze the greeting

If your email starts with a general greeting like “Valued Customer” watch out—reputable companies will often personalize the email with your first and last name.

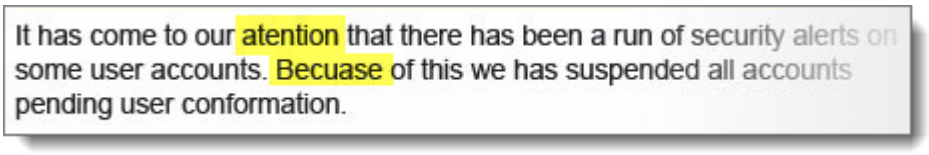


Don't trust the name or email

It’s easy for cyber criminals to fake the display name of an email and even the email address. Don’t trust them – especially if the email contains other suspicious content.

Watch out for spelling errors

Reputable companies don’t usually have major spelling mistakes or poor grammar. Read your emails carefully and report anything that seems suspicious.



Check the signature

Phishing emails often don’t include sender signatures at the end of the email. Reputable companies always provide accurate contact details.

Don't open attachments

Don’t open attachments on unexpected or “phishy” emails – these attachments often contain viruses and malware that can damage files on your computer, steal your passwords or spy on you without your knowledge.

Don't give personal information

Beware of emails that ask for you to reply with personal information or credentials (or send you to a form that requests this information).Reputable companies never ask for your personal credentials via email. Don’t give them up.

Beware of urgent language

Cyber criminals want to scare you into providing your personal information. Watch out for subject lines that claim your “account has been suspended” or your account had an “unauthorized login attempt.”

Don't believe everything

Cyber criminals are experts at fooling even the most computer-savvy individuals. Phishing emails can look nearly identical to the brands they’re pretending to be. It’s important to be skeptical with all of your email messages—if it looks even remotely suspicious, don’t open it.

REAL-WORLD PHISHING EXAMPLE

Below is an example of a Phishing email and malicious Microsoft Word attachment.