Is It a Phishing Attack?

Signs You Should Watch For & What You Should Do

1 URL

If the message you received contains a URL, hover your mouse over it. See if the address that appears matches what it should be.

WHAT YOU SHOULD DO: If Mastercard sends you an email containing a URL, the URL should start with www.mastercard.com/ ... If it starts with www.mastercard.itsnotmastercard.com/ ... watch out!

2 PERSONAL INFORMATION

Email is never the proper channel to send personal information. No one credible will ever ask you to send credit card information, social insurance numbers, or passwords via email.

WHAT YOU SHOULD DO: If you receive an email from your bank asking you for your password, call them. If the request is real, you'll get the same story over the telephone.

If you think you've received a phishing email, your colleagues may have received it as well. Please alert your IT team immediately. Don't click on anything. Don't act on any suspicious requests.

Taking phishing attacks seriously can save you or your organization a lot of time, money, credibility, and customers.

Watch for the signs.

3 EMAIL ADDRESS

The sender of an email claims to be your boss, but you don't recognize the email address. Or you do, but it's not from the company email account; it appears to be from a personal account.

WHAT YOU SHOULD DO: Validate the request with your boss before acting on it. A boss typically won't conduct business using a personal account.

4 YOUR GUT FEELING

Is an email making you feel incredibly lucky? Does it sound too good to be true? Or is an email scaring you into sending information or something catastrophic will happen?

WHAT YOU SHOULD DO: If in doubt, verify through proper channels before doing anything. Listen to the voice inside your head telling you that something isn't right.

netgovern™

Talk to one of our experts about
Data Protection and Information Governance
netgovern.com