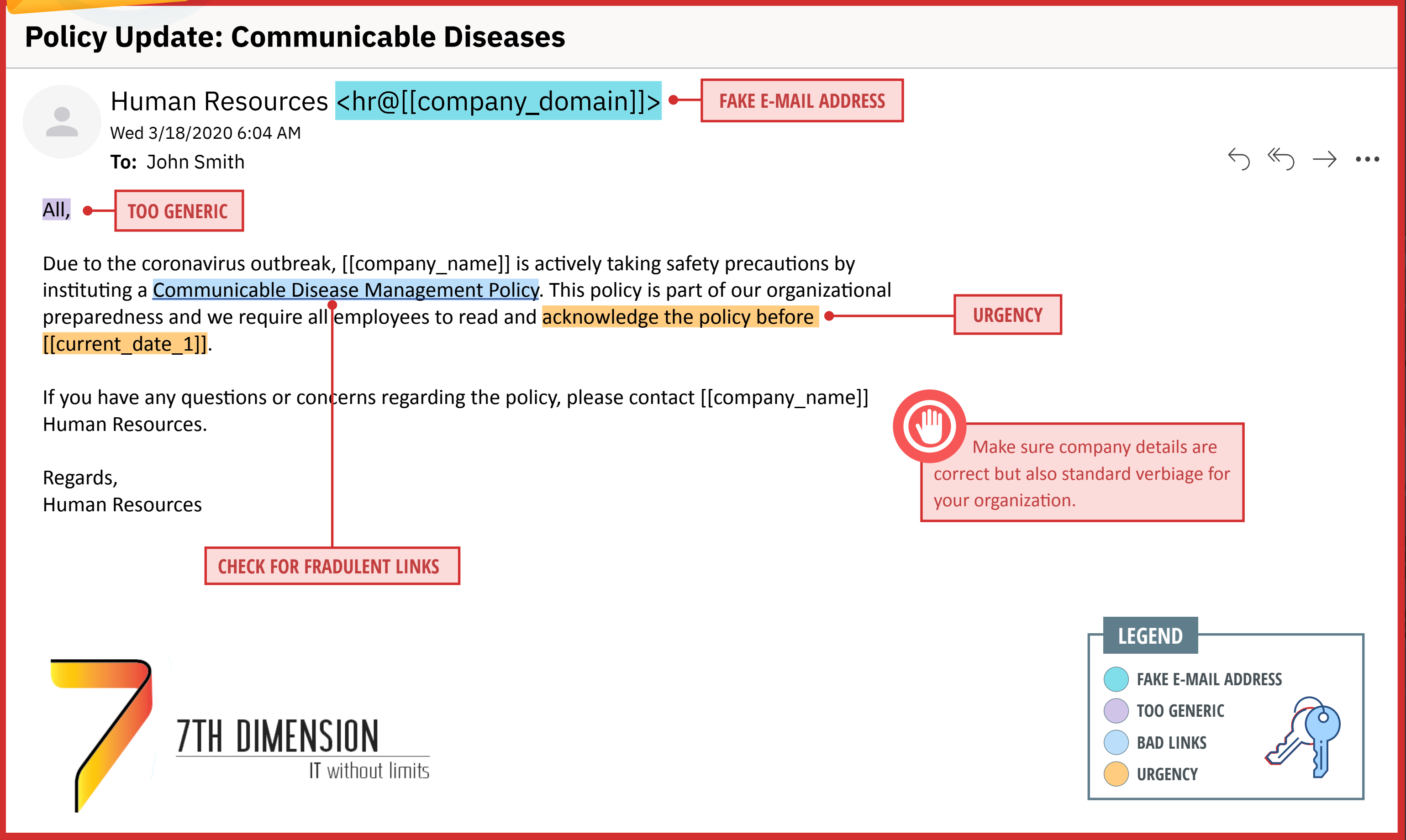
BEWARE: COVID-19 PHISHING EMAILS

EXPLOITING CONFUSED & STRESSED EMPLOYEES

Cyber criminals are exploiting headlines and global panic around the COVID-19 pandemic. Exercise extreme caution with any emails containing a COVID-19-related subject line, attachment, or hyperlinks. Be wary of social media pleas, texts, or calls related to COVID-19.



Policy Update: Communicable Diseases

Human Resources <hr@[[company_domain]]> — FAKE E-MAIL ADDRESS

Wed 3/18/2020 6:04 AM

To: John Smith

All, — TOO GENERIC

Due to the coronavirus outbreak, [[company_name]] is actively taking safety precautions by instituting a Communicable Disease Management Policy. This policy is part of our organizational preparedness and we require all employees to read and acknowledge the policy before [[current_date_1]]. — URGENCY

If you have any questions or concerns regarding the policy, please contact [[company_name]] Human Resources.

Regards,
Human Resources

CHECK FOR FRADULENT LINKS

Make sure company details are correct but also standard verbiage for your organization.

7TH DIMENSION
IT without limits

LEGEND
- 🟦 FAKE E-MAIL ADDRESS
- 🟪 TOO GENERIC
- 🟦 BAD LINKS
- 🟧 URGENCY

20 SECONDS TO BETTER EMAIL HYGIENE

1. **WATCH FOR OVERLY GENERIC CONTENT AND GREETINGS**
   Cyber criminals will send a large batch of emails. Look for examples like "Dear valued customer."

2. **EXAMINE THE ENTIRE FROM EMAIL ADDRESS**
   The first part of the email address may be legitimate but the last part might be off by letter or may include a number in the usual domain.

3. **LOOK FOR URGENCY OR DEMANDING ACTIONS**
   "You've won! Click here to redeem prize," or "We have your browser history pay now or we are telling your boss."

4. **CAREFULLY CHECK ALL LINKS**
   Mouse over the link and see if the destination matches where the email implies you will be taken.

5. **NOTICE MISSPELLINGS, INCORRECT GRAMMAR, & ODD PHRASING**
   This might be a deliberate attempt to try to bypass spam filters.

6. **CHECK FOR SECURE WEBSITES**
   Any webpage where you enter personal information should have a url with https://. The "s" stands for secure.

7. **DON'T CLICK ON ATTACHMENTS RIGHT AWAY**
   Attachments containing viruses might have an intriguing message encouraging you to open them such as "Here is the Schedule I promised."