Don't Get Hooked – Avoid Phishing

What is "phishing"?

Phishing emails look like they came from a person or organization you trust, but in reality they're sent by hackers to get you to click on or open something that will give the hackers access to your computer.

Why are you at risk?

Hackers are actively targeting our organization because we have information that is valuable to them. Specifically, they may be interested in our financial, customer, or employee data. If one employee falls for a phishing attack, our organization's entire system can potentially be accessed.

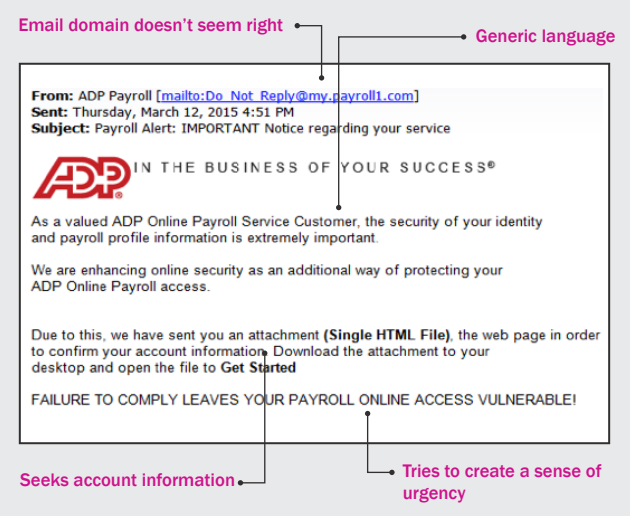
How to spot a phishing email

Hackers have gotten clever in how they design the emails they send out to make them look legitimate. But phishing emails often have the following characteristics:

- Ask you for your username and password, either by replying to the email or clicking on a link that takes you to a site where you're asked to input the information.

  IMPORTANT: Nobody at our organization will ever ask you for your password
- Look like they come from the HR or IT department
- Have grammatical errors
- Contain email addresses that don't match between the header and the body, are misspelled (like @gmaill.com), or have unusual formats (@ourcompany-othersite.com)
- Have links or email addresses that show a different destination if you hover over them
- Try to create a sense of urgency about responding.

Here is an example of a recent phishing email:



What you should do if you get a suspicious email

If you suspect that an email is a phishing email:

- Do not open any links or attachments in the email
- Notify our IT department
- **If you've already opened a link or attachment, disconnect your computer from the internet but do not turn it off and then immediately call IT.**