

# DON'T GET HOOKED AVOID PHISHING

## WHAT IS "PHISHING"?

Phishing is a type of cybercrime that uses emails disguised as coming from a person or organization you trust, in order to lure you into clicking a fraudulent link or providing access to sensitive information.

## WHY ARE YOU AT RISK?

Hackers are actively targeting your organization because you have information that is valuable to them. They may be after your customer, patient, student, or employee data. They could also be interested in your intellectual property, financial account information, or payment card data. If one employee falls for a phishing attack, your entire system may be at risk.

## 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 your IT or Information Security department immediately



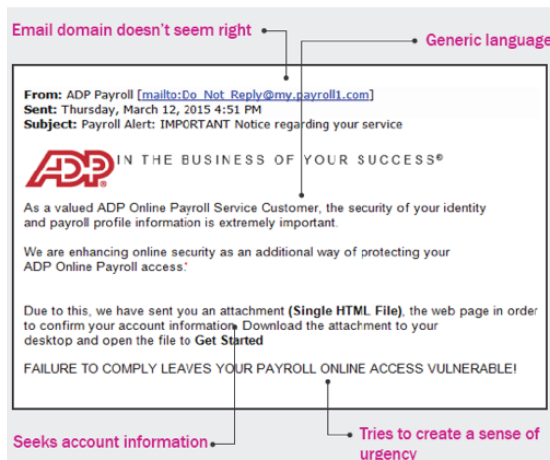
## HOW TO SPOT A PHISHING EMAIL

When hackers send out phishing emails, they try to make them look legitimate. It's important to stay vigilant and keep an eye out for these red flags:

- The email includes a request for your username and password, either by replying directly to the email or by clicking on a link that takes you to a site where you're asked to input your information. **No one in your organization should ever ask you for your password.**
- The email appears to have been sent from the HR or IT department, but something doesn't look quite right.
- There are grammatical errors in the email or subject line.
- You do not know the sender, and the email has an unexpected attachment.
- The email contains email addresses that don't match between the header and the body, are misspelled (**like @gmail.com**), or have unusual formats (**@company-othersite.com**).
- The email includes links or email addresses that, when you hover over them, list a different destination than described.
- They try to create a sense of urgency in order to get you to respond.



## HERE IS AN EXAMPLE OF A PHISHING EMAIL



The screenshot shows an email from ADP Payroll with the following details:

- From:** ADP Payroll [mailto:Do\_Not\_Reply@my.payroll1.com]
- Sent:** Thursday, March 12, 2015 4:51 PM
- Subject:** Payroll Alert: IMPORTANT Notice regarding your service

The email body contains the ADP logo and the text: "IN THE BUSINESS OF YOUR SUCCESS®". Below this, it states: "As a valued ADP Online Payroll Service Customer, the security of your identity and payroll profile information is extremely important. We are enhancing online security as an additional way of protecting your ADP Online Payroll access:"

The email then says: "Due to this, we have sent you an attachment (Single HTML File), the web page in order to confirm your account information. Download the attachment to your desktop and open the file to **Get Started**".

At the bottom, it reads: "FAILURE TO COMPLY LEAVES YOUR PAYROLL ONLINE ACCESS VULNERABLE!".

Annotations on the screenshot point to several red flags:

- Email domain doesn't seem right:** Points to the email address in the header.
- Generic language:** Points to the general security notice text.
- Seeks account information:** Points to the request to download and open an attachment.
- Tries to create a sense of urgency:** Points to the bolded "Get Started" and the warning at the bottom.

westernalliancebank.com | (800) 764-7619

Alliance Bank  
OF ARIZONA

BANK OF  
NEVADA

BridgeBank

FIRST  
INDEPENDENT  
BANK

TORREY  
PINES  
BANK

Alliance  
Association  
Bank

Divisions of Western Alliance Bank. Member FDIC.

Forbes 2020  
BEST BANKS  
IN AMERICA

Western Alliance Bancorporation has ranked in the top 10 on the *Forbes* Best Banks in America list for five consecutive years, 2016-2020.