The Employee's Guide To

PHISHING EMAILS

Identifying and Avoiding Becoming Victim to Malicious Emails That Look Genuine

Brought to you by IT Service ArchiTechs, LLC

What is a Phishing email?

Phishing is an online scam where a cyber-criminal sends an email to someone at a company, asking them to provide sensitive information, make a payment to a fraudulent account, or even a more creative objective, like purchasing gift cards and sending the serial numbers.

Many times the scammer will ask the recipient to click a link within the email, which then directs the user to a fraudulent website waiting to harvest their information or collect a payment, but it can also ask the user to simply respond to the email with the sensitive information in the response.


[redacted]
13 July 2016 at 9:38 AM
IJ
To: [redacted]
Reply-To: [redacted]
Payment

Hi Michael,

Please find enclosed vendor banking instructions for a payment that was suppose to go out in the previous week. I need you to process it immediately.

I am a bit busy now but will give you a call within the hour regarding the payment.

Regards,

[redacted]

Sent from my Mobile

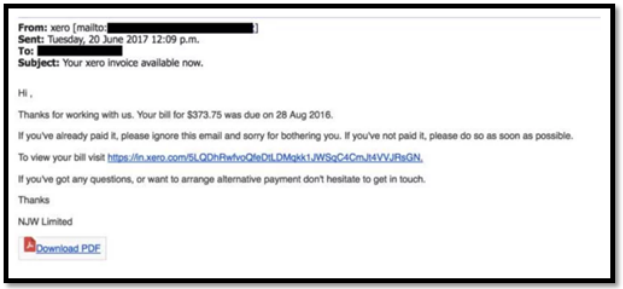
A common phishing attempt will ask the employee to make a wire transfer to a fraudulent account.

What does a Phishing email look like?

While many people assume phishing emails will be easy to spot because they'll come in the form of generic scams, like fake IRS requests, today's cybercriminals have become a little savvier.

Yes, your generic IRS request or fake PayPal request is still a popular phishing scam, but nowadays phishing scams are conducted with much more research.

The emails can look like they are coming from a coworker, and they may even have other co-workers cc'd to them. Phishing emails may even have the signature of the sender that they are trying to mimic.



From: xero [mailto:[redacted]]
Sent: Tuesday, 20 June 2017 12:09 p.m.
To: [redacted]
Subject: Your xero invoice available now.

Hi ,

Thanks for working with us. Your bill for $373.75 was due on 28 Aug 2016.

If you've already paid it, please ignore this email and sorry for bothering you. If you've not paid it, please do so as soon as possible.

To view your bill visit https://in.xero.com/5LQDhRwfvoQfeDtLDMqkk1JWSqC4CmJt4VVJRsGN.

If you've got any questions, or want to arrange alternative payment don't hesitate to get in touch.

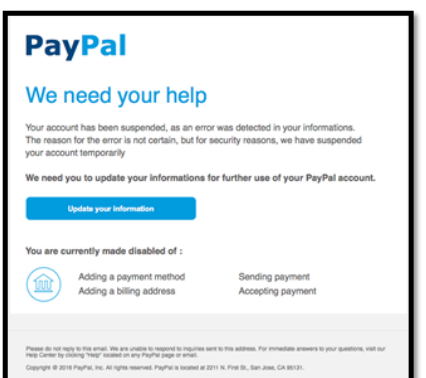
Thanks

NJW Limited

Download PDF

Sometimes the phishing attempt comes in the form of a fake invoice from what appears to be one of your vendors.

Sometimes they appear to come from a bank or other institution asking you to update your personal information.



PayPal

We need your help

Your account has been suspended, as an error was detected in your informations. The reason for the error is not certain, but for security reasons, we have suspended your account temporarily

We need you to update your informations for further use of your PayPal account.

Update your information

You are currently made disabled of :

Adding a payment method
Adding a billing address
Sending payment
Accepting payment

Please do not reply to this email. We are unable to respond to inquiries sent to this address. For immediate answers to your questions, visit our Help Center by clicking "Help" located on any PayPal page or email.

Copyright © 2016 PayPal, Inc. All rights reserved. PayPal is located at 2211 N. First St., San Jose, CA 95131.

What should you do if you suspect a Phishing email?

The good news is, protecting yourself from being a victim is pretty straightforward. If you get an email that looks suspicious, here are three easy ways to check if the email is real or if it's a phishing scam:

1) Contact the sender – if the phishing attempt is meant to look like it's from a colleague or boss, simply call that person on the phone, walk over to their desk, or send them an email (outside of the email thread with the phishing attempt) and ask if they sent you something. If the phishing attempt appears to have come from a company, contact that company and ask them if they really requested the information.

2) Double check the "reply-to" or website address – when the Phishing attempt is asking for the sensitive data directly as a response to the email, they will have a reply-to address from a domain that is not the actual domain name of the sender. If the email is sending you to a website to collect the information or payment, the domain won't be the official domain of that company.

3) Ask us – helping with computer issues is exactly what we're here for. We'd much rather get a call from you asking to double-check a suspicious email, than a call saying that your system is locked up from a ransomware attack that came from clicking the link in that email.

Closing out

The important thing to remember about phishing emails is that it's always better to double-check if you're unsure. It's much easier to simply ask the supposed sender if they actually sent it than to deal with the consequences of being the victim later on.

If you have any questions about phishing emails or other IT-related inquiries, please do not hesitate to contact us directly. Reach out to David Appelbaum, Director of Strategic Partnerships at ArchiTechs, to schedule a "getting to know you" consultation.

David Appelbaum
david@itsasupport.com
610-543-1500

IT Service ArchiTechs, LLC
80 Maple Ave Floor 1, Media, PA 19063
T: 610-543-1500