

PIMA COUNTY Cyber Security Quarterly

Pima County's Cyber Security Team, bringing you information and tips for a safe, available and confidential environment.

April-July, 2019

Phishing is on the Rise-- and It's Not Going to Stop

We hear the term "Phishing" all the time, but what exactly is it? If you believe that is a term that only applies in the world of cyber security professionals, then consider this:

Today's attackers employ a variety of deception tactics allowing them to impersonate legitimate users and bypass existing IT security defenses. Web applications are often compromised in order to host malware or be turned into a phishing site. Users who visit these sites then become infected or have their credentials stolen, giving attackers access to your network. Once inside, attackers use stealthy techniques to move around the network looking for targets, while remaining undetected, sometimes for months. (Source: <https://www.infosecurity-magazine.com>)

Phishing is the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

Spear Phishing goes further by targeting very specific individuals, organizations or businesses.

*** It is important to note that phishing victims are not just targeted at their place of work. While Pima's Information Security Team diligently protects your work environment by preventing most phishing emails from even reaching your inbox, some will inevitably get through. Any cyber threat that exists on our network can exist on any network including yours at home.***

- **Phishing emails are designed to make you panic**
- **Phishing emails often look like they are from a company you know or trust**
- **When in doubt, throw it out!**



What You Should do When You Suspect a Phishing Attempt

1. Recognize what it is: if it looks fishy it is phishy
2. Do not click on anything that you suspect to be malicious or anything unexpected in your inbox asking for credentials
3. Report it as spam by either clicking the "Report Phishing Email" button in Outlook or forwarding the email to spam@pima.gov.
4. If you accidentally clicked on any link that you believe to be suspicious, immediately report it to the NOC @ 724-8741.

A Few More Things to Consider

- If you get an email asking you to click a link or open an attachment, ask yourself this question: **Do I have an account with this company or know the person who contacted me? If so, was I expecting it?**

- Phishing emails often tell a story to trick you into clicking a link or opening an attachment. They may:
 - >> Say they've noticed suspicious activity or log-in attempts
 - >> Claim there is a problem with your account or payment information
 - >> Say you must confirm some personal information
 - >> Include a fake invoice
 - >> Want you to click a link to make a payment

90%

90% of organizational data breaches is attributed to successful phishing

76% of businesses reported being a victim of a phishing attack in the last year

76%

Test Your Phishing Knowledge

Take a look at the two phishing examples below and see if you can figure out why they are suspicious. Answers are on page 3.

1

Warning - Your System will be Shutdown !

 Apple ID <no-reply@supportmail.apple.com>
Wed 7/17/2019 12:13 PM
To: [redacted] &

This message and sender come from outside Pima County. If you did not expect this message, proceed

This is an automated email, please do not reply

Dear Client

Please confirm your billing informations to gives you easy access to a variety of Apple services. Verification is required to protect your account information and helps us serve you better remember if you will not update your billing information we will disable and suspend your apple system operator service on your device and you won't be able to use it anymore Please Verify your account information by clicking on the link below

[Click here to Verify your ID](#) zkmnsyh.com/wed/

Thanks for choosing Apple,
Apple Team

© 2019 Apple. All rights reserved.

Email ID: 163327

2

NETFLIX

⚠ Your account is on hold.

Please update your payment details

Hi Dear,

We're having some trouble with your current billing information. We'll try again, but in the meantime you may want to update your payment details.

[UPDATE ACCOUNT NOW](#)

Need help? We're here if you need it. Visit the [Help Centre](#) or [contact us](#) now.

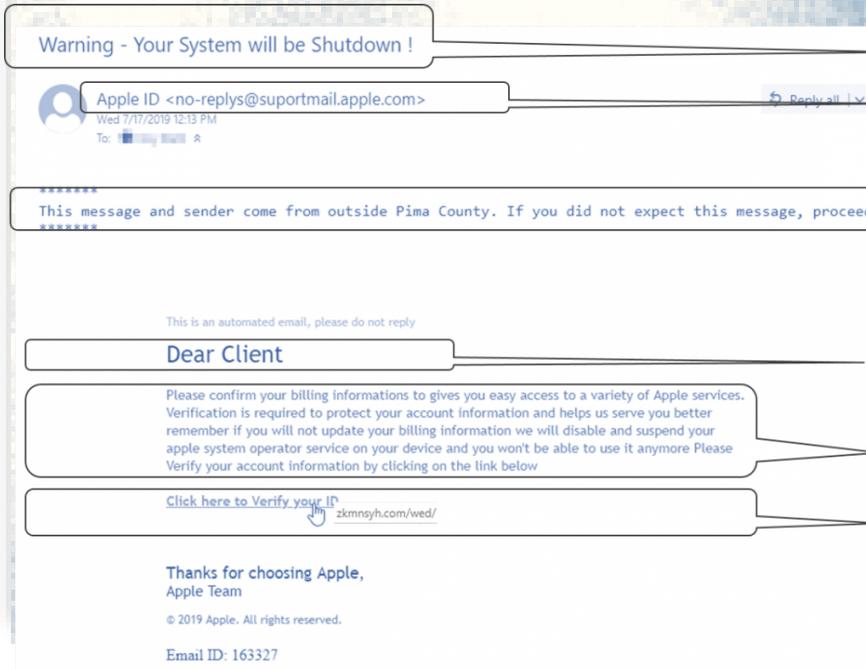
- Your friends at Netflix

Questions? Call 1800 098 8879

Test Your Phishing Knowledge

Answers

1



The attention grabber

Misspellings

Always look more closely at email originating from outside of Pima

It is unlikely Apple would address users this way

Rampant misspellings, poor grammar

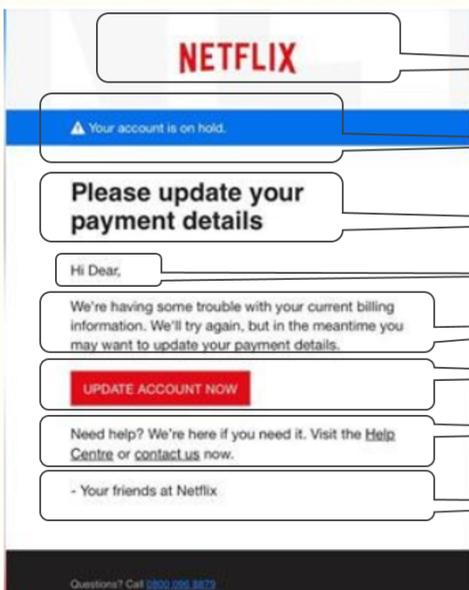
Hovering your cursor over the hyperlink shows a suspicious looking website

RED FLAGS

- Look for an attention grabber that doesn't make sense: Apple would not shut down a system or account in this manner
- One misspelling is unexpected in a professional email, but this many is a huge red flag
- There is no phone number to actually contact a person with questions



2



The Trust Factor: You trust NETFLIX, right?

The Trick: Calling you into action

The Claim: Calling you into action

Pay Attention: How likely is it that NETFLIX would call you "Dear"?

The Problem Statement: Update your payment info

It's Too Late!: If you've clicked, you may have been redirected to a malicious site or possibly unknowingly started a "drive by" download of malicious code

Same!: Any of these links could be malicious. If they didn't get you before, here is another chance

These people are not your friends! Remember, friends don't phish friends.

RED FLAGS

- Generally, no reputable company would ask for payment updates in this way
- There is no phone number to actually contact a person with questions
- If you are suspicious, go to the actual customer service portal for the company and ask if they sent the email

