5 Types of Social Engineering Scams to Know:

1 Phishing:

The leading tactic leveraged by today's ransomware hackers, typically delivered in the form of an email, chat, web ad or website designed to impersonate a real system and organization. Often crafted to deliver a sense of urgency and importance, the message within these emails often appears to be from the government or a major corporation and can include logos and branding.

2 Baiting:

Similar to phishing, baiting involves offering something enticing to an end user in exchange for private data. The "bait" comes in many forms, both digital, such as a music or movie download, and physical, such as a branded flash drive labeled "Executive Salary Summary Q3 2016" that is left out on a desk for an end user to find. Once the bait is taken, malicious software is delivered directly into the victim's computer.

3 Quid Pro Quo:

Similar to baiting, quid pro quo involves a request for the exchange of private data but for a service. For example, an employee might receive a phone call from the hacker posed as a technology expert offering free IT assistance in exchange for login credentials.

4 Pretexting:

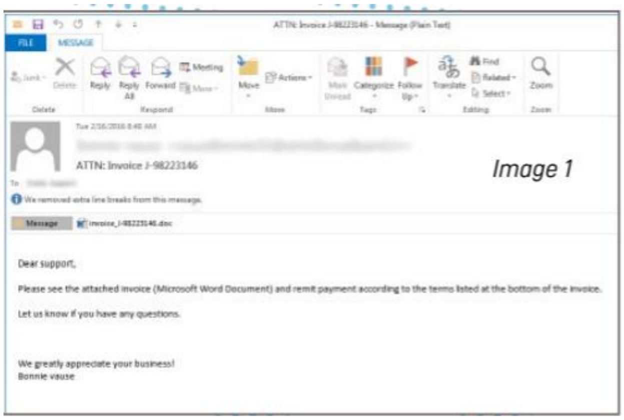
When a hacker creates a false sense of trust between themselves and the end user by impersonating a co-worker or a figure of authority within the company in order to gain access to private data. For example, a hacker may send an email or a chat message posing as the head of IT Support who needs private data in order to comply with a corporate audit (that isn't real).

5 Tailgating:

When an unauthorized person physically follows an employee into a restricted corporate area or system. The most common example of this is when a hacker calls out to an employee to hold a door open for them as they've forgotten their RFID card. Another example of tailgating is when a hacker asks an employee to "borrow" a private laptop for a few minutes, during which the criminal is able to quickly steal data or install malicious software.

Takeaway: Employee awareness of social engineering is essential for ensuring corporate cybersecurity. If end users know the main characteristics of these attacks, it's much more likely they can avoid falling for them. As many of us are visual learners, make sure to provide them with actual examples of these scams.

5 Types of Social Engineering Scams to Know:



Tue 2/16/2016 8:48 AM
[redacted]
ATTN: Invoice J-98223146
To [redacted]
We removed extra line breaks from this message.
invoice_J-98223146.doc

Dear support,

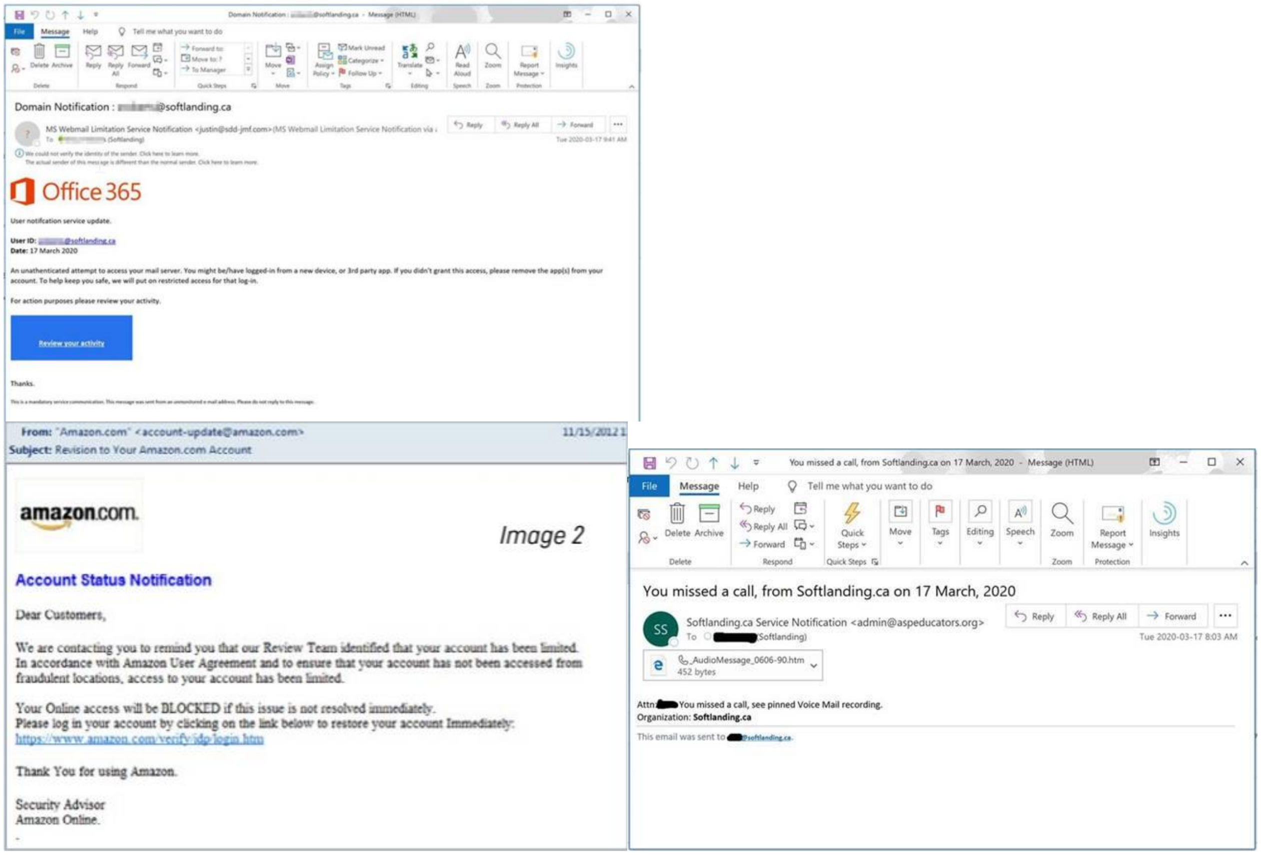
Please see the attached invoice (Microsoft Word Document) and remit payment according to the terms listed at the bottom of the invoice.

Let us know if you have any questions.

We greatly appreciate your business!
Bonnie vause

Image 1

Image 1 is a prime example of a phishing email used to spread Locky, a common strain of ransomware. To the recipient, the email appears to come from a business partner asking the reader to “see the attached invoice” by clicking on the attached Word doc or a security alert for you to review and another about a missed call with an attachment that appears to be a voicemail/audio file. Note how harmless this email appears and how easy it would be for a user to absentmindedly open and click, an action that would result in an instant ransomware infection. It happens every single day.



Domain Notification : [redacted]@softlanding.ca

MS Webmail Limitation Service Notification <justin@sdd-jmf.com> (MS Webmail Limitation Service Notification via ...
To [redacted] (Softlanding)
Tue 2020-03-17 9:41 AM

We could not verify the identity of the sender. Click here to learn more.
The actual sender of this message is different than the normal sender. Click here to learn more.

User notifcation service update.

User ID: [redacted]@softlanding.ca
Date: 17 March 2020

An unathenticated attempt to access your mail server. You might be/have logged-in from a new device, or 3rd party app. If you didn't grant this access, please remove the app(s) from your account. To help keep you safe, we will put on restricted access for that log-in.

For action purposes please review your activity.

Thanks.

This is a mandatory service communication. This message was sent from an unmonitored e-mail address. Please do not reply to this message.

From: "Amazon.com" <account-update@amazon.com> 11/15/2012 1
Subject: Revision to Your Amazon.com Account

Account Status Notification

Dear Customers,

We are contacting you to remind you that our Review Team identified that your account has been limited. In accordance with Amazon User Agreement and to ensure that your account has not been accessed from fraudulent locations, access to your account has been limited.

Your Online access will be BLOCKED if this issue is not resolved immediately.
Please log in your account by clicking on the link below to restore your account Immediately:
https://www.amazon.com/verify/idp/login.htm

Thank You for using Amazon.

Security Advisor
Amazon Online.

You missed a call, from Softlanding.ca on 17 March, 2020

SS Softlanding.ca Service Notification <admin@aspeducators.org>
To [redacted](Softlanding)
Tue 2020-03-17 8:03 AM

_AudioMessage_0606-90.htm
452 bytes

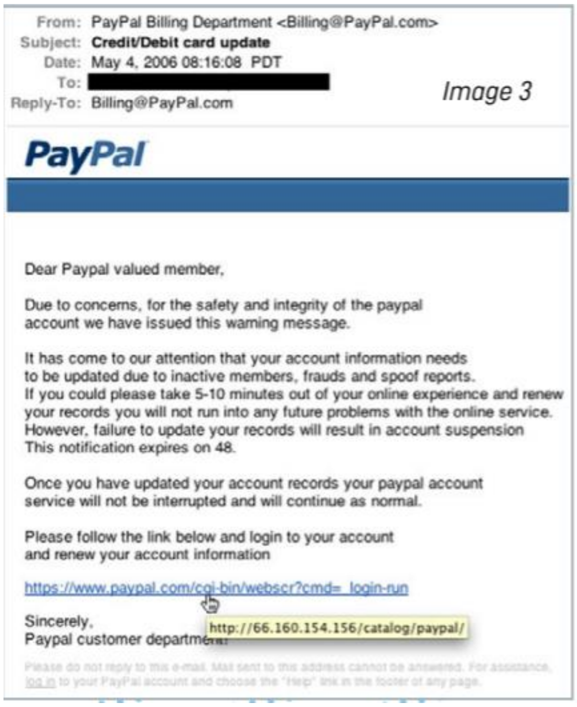
Attn:[redacted]You missed a call, see pinned Voice Mail recording.
Organization: **Softlanding.ca**

This email was sent to [redacted]@softlanding.ca.

Image 2

Above is another example of an email scam, which appears to be an official notice from Amazon.com and lures the reader to click a link rather than an attachment, but with the same business-crippling results.

5 Types of Social Engineering Scams to Know:



From: PayPal Billing Department <Billing@PayPal.com>
Subject: **Credit/Debit card update**
Date: May 4, 2006 08:16:08 PDT
To: [redacted]
Reply-To: Billing@PayPal.com

Dear Paypal valued member,

Due to concerns, for the safety and integrity of the paypal account we have issued this warning message.

It has come to our attention that your account information needs to be updated due to inactive members, frauds and spoof reports.
If you could please take 5-10 minutes out of your online experience and renew your records you will not run into any future problems with the online service.
However, failure to update your records will result in account suspension
This notification expires on 48.

Once you have updated your account records your paypal account service will not be interrupted and will continue as normal.

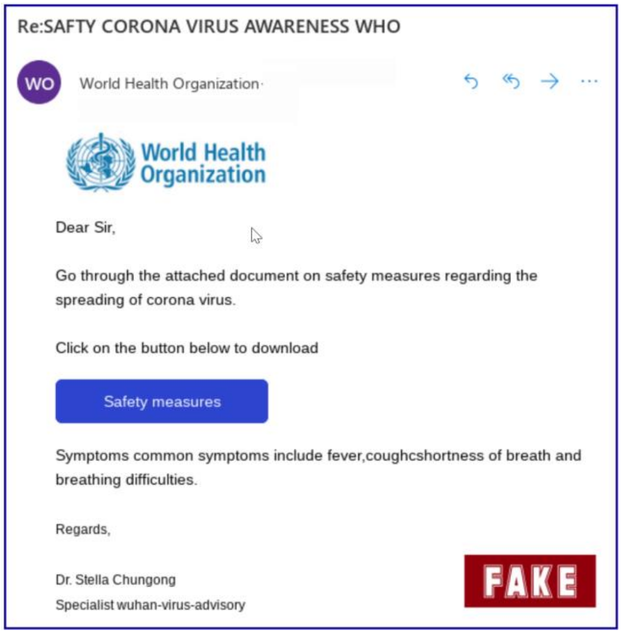
Please follow the link below and login to your account and renew your account information

https://www.paypal.com/cgi-bin/webscr?cmd=_login-run

http://66.160.154.156/catalog/paypal/

Sincerely,
Paypal customer department

Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, log in to your PayPal account and choose the "Help" link in the footer of any page.



Re:SAFTY CORONA VIRUS AWARENESS WHO

WO World Health Organization

Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus.

Click on the button below to download

Symptoms common symptoms include fever,coughcshortness of breath and breathing difficulties.

Regards,

Dr. Stella Chungong
Specialist wuhan-virus-advisory

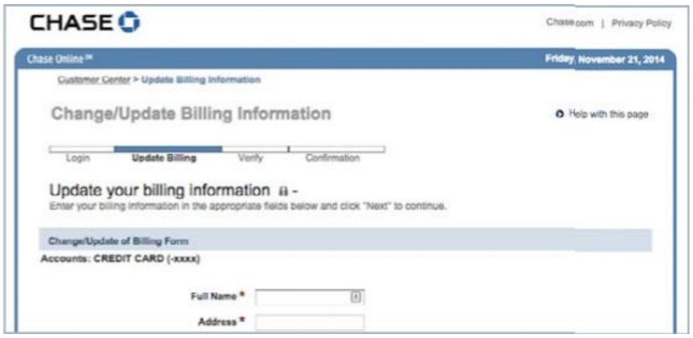
Image 3

In image 3, note the link appears to direct the reader to a legitimate PayPal web page and yet, when the mouse is hovered over the link, you see that it actually directs to a different site designed to inject malware or illegally collect personal information. Also the recent emails that appear to be from WHO with information on the corona virus. If it is not an organization you would expect to receive an email from be cautious and verify.

Red flags: Missing sender or recipient information, generic greetings, misspelled email addresses (i.e., billing@amzaon.com), and email addresses that don't match the company name. Any emails that ask the recipient to download a form or macro in order to complete a task are highly suspicious and an employee should NOT click on anything. Instead, report the email to IT immediately.

Malicious Websites and Malvertising: Malicious websites and malvertisements are designed to look like a page or ad on a legitimate website. These sites can look incredibly real, featuring branding and logos, which is why so many end up giving cyber criminals their personal information or access to directly inject malware onto their systems. Typically, hackers will insert code into a legitimate site which redirects unsuspecting users to their malicious site. Below, you'll find an example of a malicious page that was designed to look like a page on Chase Bank's site along with a recent pop up to enter your email address and password to get more information on the corona virus. You do not need to enter your email credentials outside of Office 365 or your computer.

5 Types of Social Engineering Scams to Know:



CHASE

Chase.com | Privacy Policy

Chase Online℠

Friday, November 21, 2014

Customer Center > Update Billing Information

Change/Update Billing Information

Help with this page

Login | Update Billing | Verify | Confirmation

Update your billing information 🔒 -

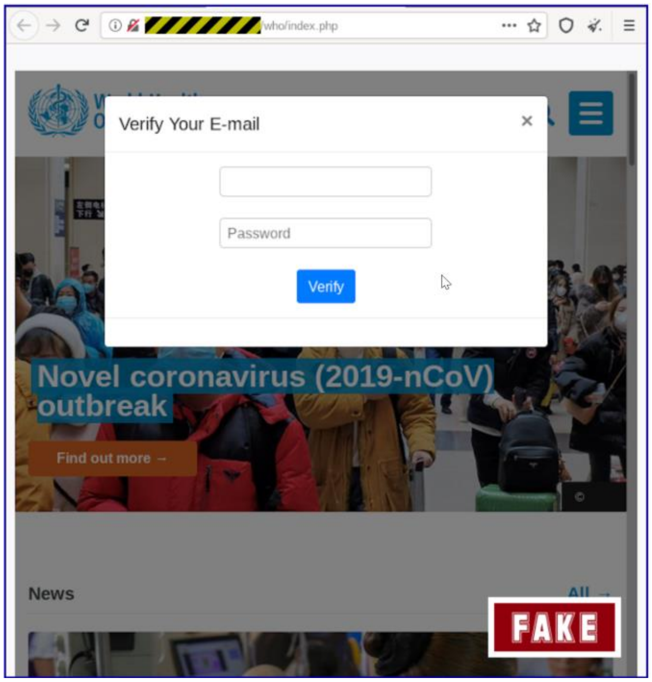
Enter your billing information in the appropriate fields below and click "Next" to continue.

Change/Update of Billing Form

Accounts: CREDIT CARD (-xxxx)

Full Name *

Address *



[redacted]who/index.php

Verify Your E-mail ×

Password

Verify

Novel coronavirus (2019-nCoV) outbreak

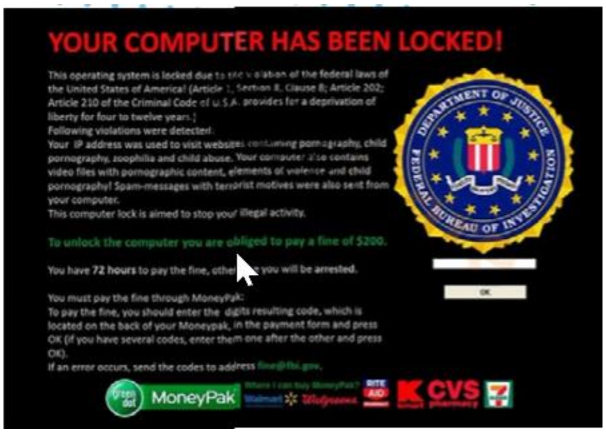
Find out more →

News

All →

FAKE

Pop Ups Another common lure is a pop-up that claims that a user's computer has been locked by the FBI because it was used to access illegal material such as child pornography, as you will see in the example above. The lure instructs users to click a link in order to pay a fine, which is bogus. Red flags: Links that redirect to a different domain, pop-ups that require you to enter personal information, misspelled URLs, and URLs with unusual domain extensions. This type of attack can be very hard to detect, even if employees are highly vigilant.



YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

You have 72 hours to pay the fine, otherwise you will be arrested.

You must pay the fine through MoneyPak:
To pay the fine, you should enter the digits resulting code, which is located on the back of your Moneypak, in the payment form and press OK (if you have several codes, enter them one after the other and press OK).
If an error occurs, send the codes to address fine@fbi.gov.

Lastly also be cautious of phone calls and verify the caller if they are asking for information or for you to confirm information. If uncertain of the caller let them know you will call them back and call back the number on the appropriate website – this is a common one from the CRA. Do not call back the number that called you.