CYNERGISTEK

Phishing Awareness

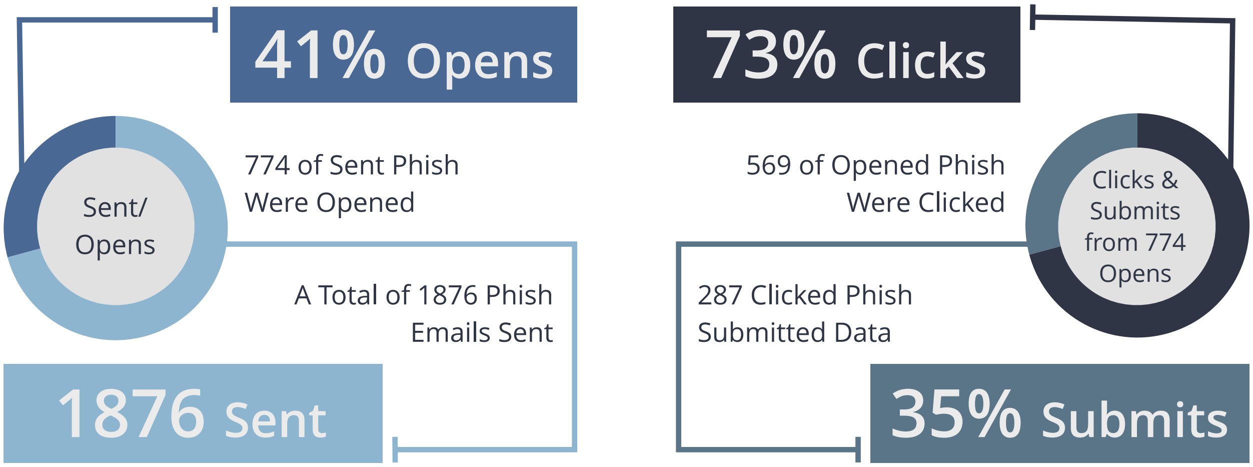
Attackers engage with you through your email inbox, and unless you pay close attention, you can become a victim to their masquerade. What tactic are these attackers using? It is called phishing and it targets your trust.

What is Phishing?

Phishing was coined to describe how attackers send uniquely crafted emails to fool you into clicking malicious URLs or downloading software payloads. Often, phish are sent in large groups and have a general salutation meant to appeal to large audiences. Sometimes an attacker puts forth extra effort to appear legitimate and will include specific elements related to the target, which is appropriately called spear phishing.

Millions of phish are pointed at inboxes daily. Most organizations implement technical controls to prevent this type of attack; however, attackers keep pace with these efforts and are continuously employing evasive techniques. The need for you to understand how to deal with them is necessary to protect your patients, organization and coworkers.

Organizations often find that employees are not well-versed in the proper method of scrutinizing email messages, putting information security at risk. In fact, CynergisTek has found that 41% of our phish assessment emails are opened and that 73% click on the link in the email.



41% Opens

774 of Sent Phish Were Opened

A Total of 1876 Phish Emails Sent

1876 Sent

73% Clicks

569 of Opened Phish Were Clicked

287 Clicked Phish Submitted Data

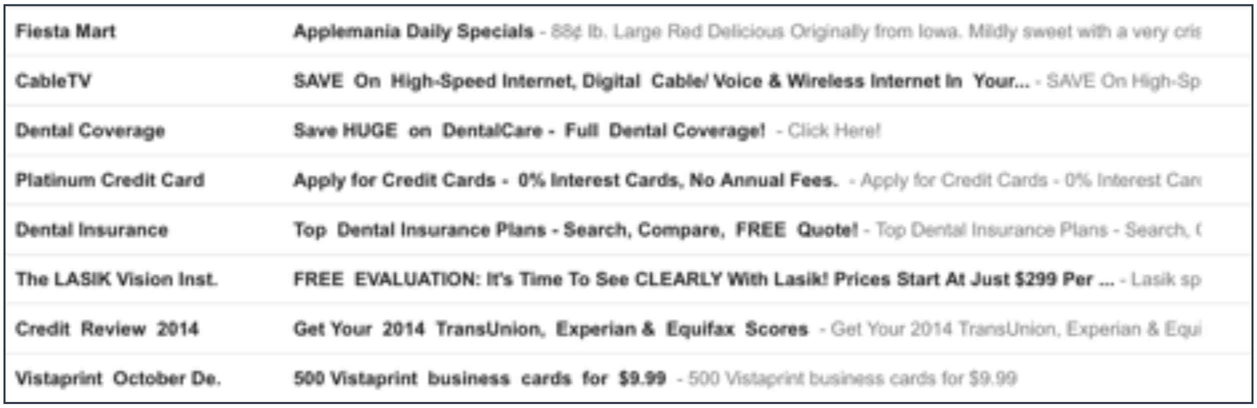
35% Submits

How Do I Identify These Types of Attacks?
The most important step to prevent phish attacks is identifying them, which is not as difficult as it may seem. By adhering to fundamental email practices, you can appropriately spot messages plying phishing tactics.

The initial item to be aware of is the most basic information an email client provides, which is the sender address. A number of questions should accompany each message, such as:

- "Who is this sender?"
- "Have I interacted with this entity before?"
- "Is the subject related to any familiar event or account?"

If you are able to answer these questions with appropriate information, opening a message might be the next step. Opening messages, especially viewing included images, should not be automatic due to the potential that these actions can trigger special attack payloads.



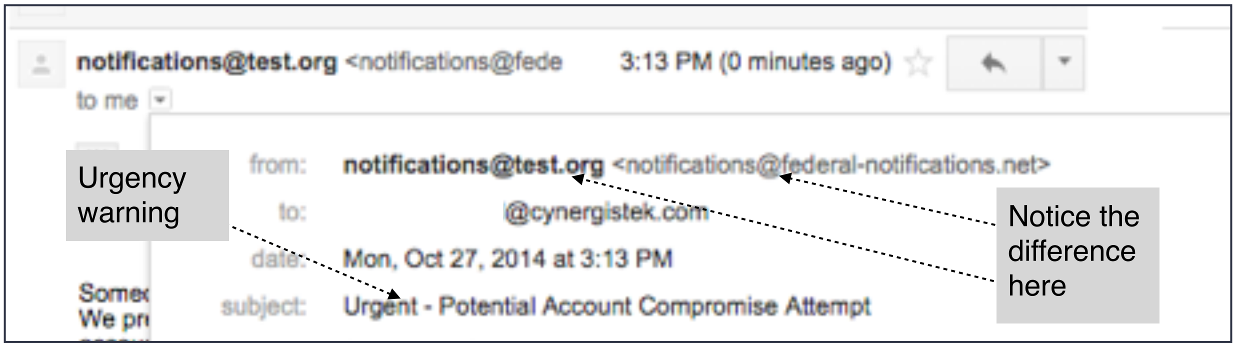
Fiesta Mart	Applemania Daily Specials - 88¢ lb. Large Red Delicious Originally from Iowa. Mildly sweet with a very cris
CableTV	SAVE On High-Speed Internet, Digital Cable/ Voice & Wireless Internet In Your... - SAVE On High-Sp
Dental Coverage	Save HUGE on DentalCare - Full Dental Coverage! - Click Here!
Platinum Credit Card	Apply for Credit Cards - 0% Interest Cards, No Annual Fees. - Apply for Credit Cards - 0% Interest Car
Dental Insurance	Top Dental Insurance Plans - Search, Compare, FREE Quote! - Top Dental Insurance Plans - Search, (
The LASIK Vision Inst.	FREE EVALUATION: It's Time To See CLEARLY With Lasik! Prices Start At Just $299 Per ... - Lasik sp
Credit Review 2014	Get Your 2014 TransUnion, Experian & Equifax Scores - Get Your 2014 TransUnion, Experian & Equi
Vistaprint October De.	500 Vistaprint business cards for $9.99 - 500 Vistaprint business cards for $9.99

After an email is opened, you should review it to identify the overall nature of the email before clicking any link. Even if the link comes from someone you recognize it should not be an automatic response to click. Always read the message and verify its authenticity before you click any links.

How can you determine the authenticity of a message? If the message looks remotely suspicious, a number of clues provided within the content can help you correctly screen phishing messages. Ask yourself the following questions to find them:

- Does the "from address" actually match the real sender's address? Sometimes attackers mask the actual sending address in order to appear legitimate from just a passing glance.

- Is this an urgent message? Attackers know you are more likely to follow a link if it seems urgent or carries a tone of importance. Messages declaring short response timeframes or displaying symbols of authority should be treated with greater suspicion.



notifications@test.org <notifications@fede 3:13 PM (0 minutes ago)
to me

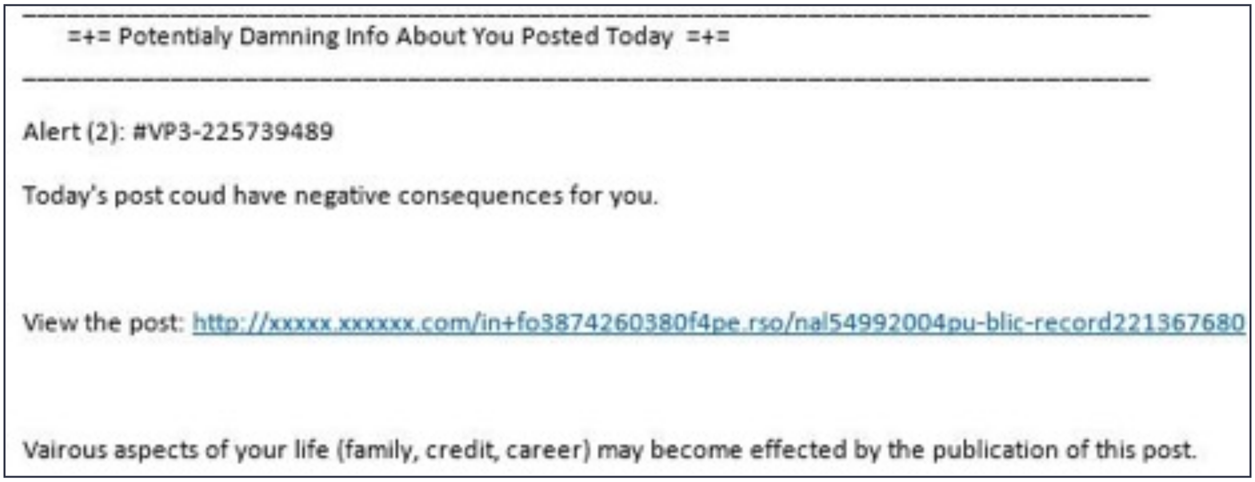
from: notifications@test.org <notifications@federal-notifications.net>
to: @cynergistek.com
date: Mon, Oct 27, 2014 at 3:13 PM
subject: Urgent - Potential Account Compromise Attempt

Some
We pr

Urgency warning

Notice the difference here

- Does your name appear in the message? Spear phish are more work to create, so generic messages sent in large batches are more common. Correspondence of importance rarely comes without legitimate identifying information about you.
- Is the content properly formatted and written? Many times messages originate from countries where authors might not be familiar with proper English syntax and spelling.



```
------------------------------------------------------------------------------------
   =+= Potentialy Damning Info About You Posted Today =+=
------------------------------------------------------------------------------------
```

Alert (2): #VP3-225739489

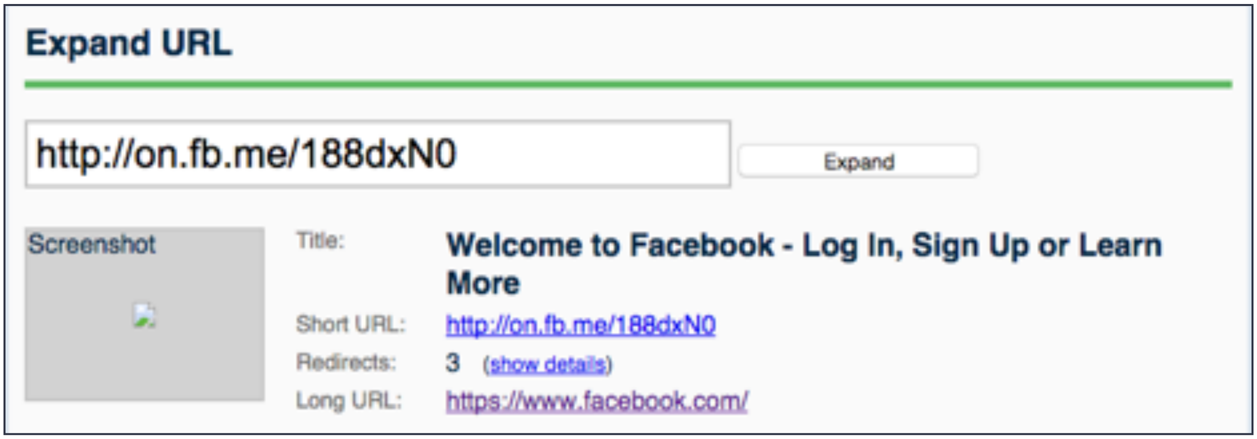
Today's post coud have negative consequences for you.

View the post: http://xxxxx.xxxxxx.com/in+fo3874260380f4pe.rso/nal54992004pu-blic-record221367680

Vairous aspects of your life (family, credit, career) may become effected by the publication of this post.

- Do search engine queries on the sender's signature line information (phone numbers or address) provide verification? While errors caught by this method only identify poorly researched phish, it is still a method of elimination.

- Does the link support encryption? Look at the beginning of the link to see if it is encrypted (https://…) before you click it. Few vendors, third parties or internal resources want protected information such as passwords submitted over unencrypted websites.
- Is the message asking for important information? Treat requests for account details with intense suspicion. Security or administrators often have access to account details and they do not need them from you. Reiterating and underlining, passwords should never be given out.
- Does the text of the link match the actual link? Hover over links to display the actual intended destination because what appears to be domain.com could be something else entirely.
- Has the link been shortened? Link shortening services sometimes mask the address of a phishing link. Expand these URLs using web resources (e.g., LongURL.org) if they appear suspicious.



Expand URL

http://on.fb.me/188dxN0

Title: Welcome to Facebook - Log In, Sign Up or Learn More
Short URL: http://on.fb.me/188dxN0
Redirects: 3 (show details)
Long URL: https://www.facebook.com/

- Is the message requesting a file download? Attachments with common extensions should be treated with extreme suspicion before clicking them (e.g., .exe, .doc, .xls, .pdf, .zip, etc.).

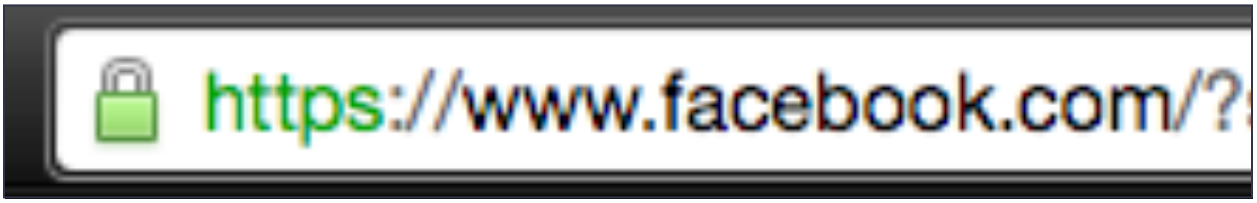
What Should I Do If I Receive a Suspicious Message?

If any indicators of phishing are discovered, you should immediately notify the appropriate staff within your organization. Under no circumstances forward a phish, and if ever instructed, include the phish as an attachment only. Delete phish after you receive acknowledgement of your report and are told to do so.

If you click a link within a phish, you might still have a chance to avoid a huge mistake. While it is true attackers can run malicious code within links, many times they are after information you submit to them after clicking their link.

Look closely at the landing page whenever you are brought to a website after clicking an email link and perform the following actions:

- Check the quality of the page. Phishing pages are often quickly created and lack dynamic features of the ones they mimic. Lack of external links, company banners or logos are telltale signs of illegitimacy.
- Review the URL of the page even if it has HTTPS protections. A page like 123.45.6.789/domain/security-helper.com is not the same as a page from the www.security-helper.com domain.
- Verify if the webpage asks for authentication on a secure page. You should never submit information (especially passwords) requested via an unencrypted website. Only URLs with the https:// prefix and the secure padlock icon should be used for authentication webpages.



https://www.facebook.com/?

Don't Be the Victim of a Phishing Attack
If all of these tips are followed, the likelihood that you will fall victim to a phishing attack is significantly decreased and thus reduces the risk for potential account compromise, security incidents and other serious events. Remain vigilant when interacting with your inbox and you'll protect patients, your organization and yourself from harm.

You can also test your organization's phishing knowledge with one of CynergisTek's customized phishing assessments and improve your organization's awareness. Our assessment is a great training experience that can improve your organization's security program. To find out more on how your organization can reduce the risk of a phishing attack, visit http://cynergistek.com/technical/se/ or email info@cynergistek.com.