

When Hackers go Phishing: Don't Become a Victim



Introduction – Jim Murphy, City of Quincy

- Director of Information Technology
- Financial Oversight of Self-funded Health Insurance Plan
- Credentials:
 - Masters Business Administration
 - Certified Information Security Manager
 - Certified Government Chief Information Officer
 - Certified HIPPA Privacy Security Expert
 - Numerous courses & trainings in information security and regulatory compliance
- Adjunct Instructor at Quincy University

Why are we here?



- Cyber security Threats – What keeps I.T. Directors up at night!
- Ransomware – Do we really need to worry?
- Why does Finance need to take an active role in security?
- Why employees can make or break any cyber security program?
- Become familiar with how to identify Phishing techniques.

Government Regulations

What Keeps Government I.T. Directors Awake at Night!



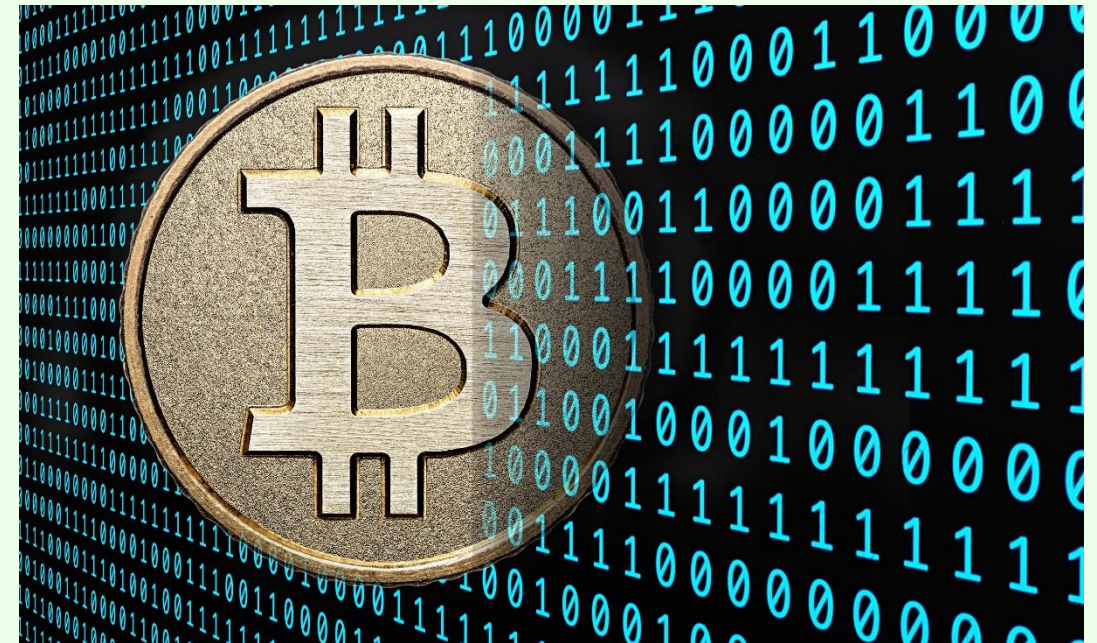
What is Ransomware!

Ransomware is a form of malware in which rogue software code effectively holds a user's computer hostage until a "ransom" fee is paid. **Ransomware** often infiltrates a PC as a computer worm or Trojan horse that takes advantage of open security vulnerabilities.



Source: www.webopedia.com

Ransomware – The Darkweb & Bitcoins



Why should you care about security? Isn't that what I.T. gets paid to do?

April 28, 2016

Cyberattack knocks Lansing utility offline

Town of Palm Beach fights ransomware attack on 911 system

City computers infected with virus

By [Anna Erickson](#) on Jul 29, 2016 at 12:08 a.m.

Ransomware Crooks Demand \$70,000 After Hacking San Francisco Transport System -- UPDATED

Ransomware attack on San Francisco public transit gives everyone a free ride

City of Sarasota's system hacked by ransomware, data held hostage

Aug 20, 2016 0

Janesville computer systems hit by virus, likely 'ransomware'

Ransomware targets Howard County government

Local office hit last week, resulting in 33,000 files being affected

Devin Zimmerman Nov 29, 2016 0

Police Department Loses Years Worth of Evidence in Ransomware Incident

By [Catalin Cimpanu](#)

January 26, 2017 11:57 AM

City of Sarasota's system hacked by ransomware, data held hostage

Aug 20, 2016 0

Henry County Hit with Ransomware, Leaving 18,000 Voters as Victims

December 8, 2016 Erin Allen

HACKERS ATTEMPT TO HOLD CAPITOL HILL DATA FOR RANSOM

Ransomware virus infects PCAO case files

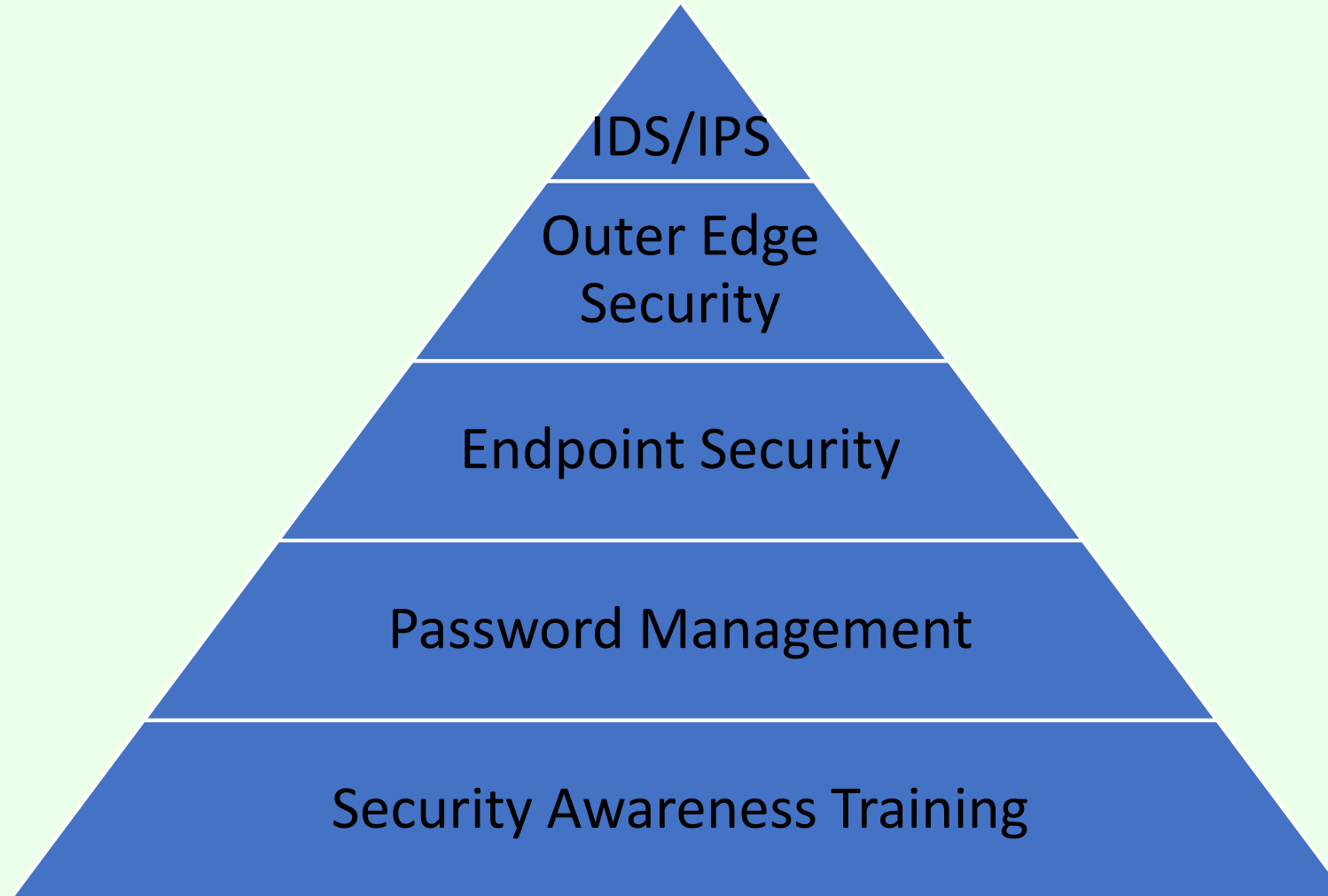
12 News , KPNX 8:42 PM: MST May 31, 2016

So are we all doomed?

Cyber Threats are becoming more sophisticated and are growing at an alarming rate. Can anything be done? YES!

- Appreciate the risk your organization is battling
- Audit the security tools, training and practices being used
- Develop or modify employment policies & procedures
- Develop a training program
- Keep systems up-to-date
- Develop and implement a information security strategy

City of Quincy Security Initiative



Define Social Engineering

Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional “con” in that it is often one of many steps in a more complex fraud scheme.

Source: Wikipedia 7/11/17



Know the Risk
Raise your Shield

SPEAR PHISHING



0:00 / 0:34



Phishing by the Numbers:

85 percent of organizations have suffered phishing attacks

#1 delivery vehicle for malware is email attachments

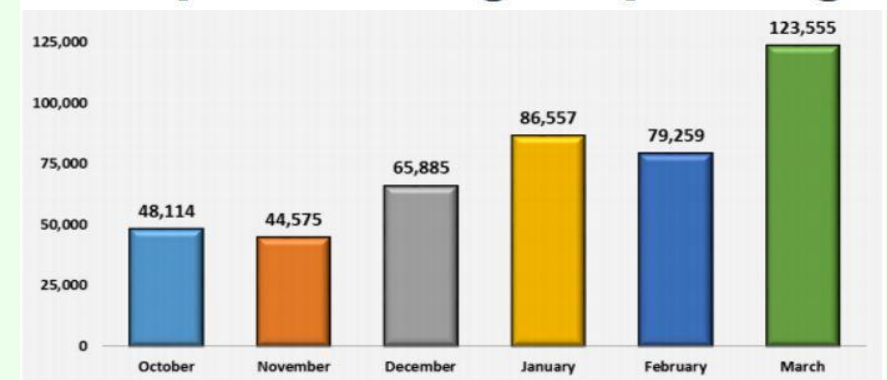
30 percent of phishing emails get opened

\$1.6 million: the average cost of a spear phishing attack

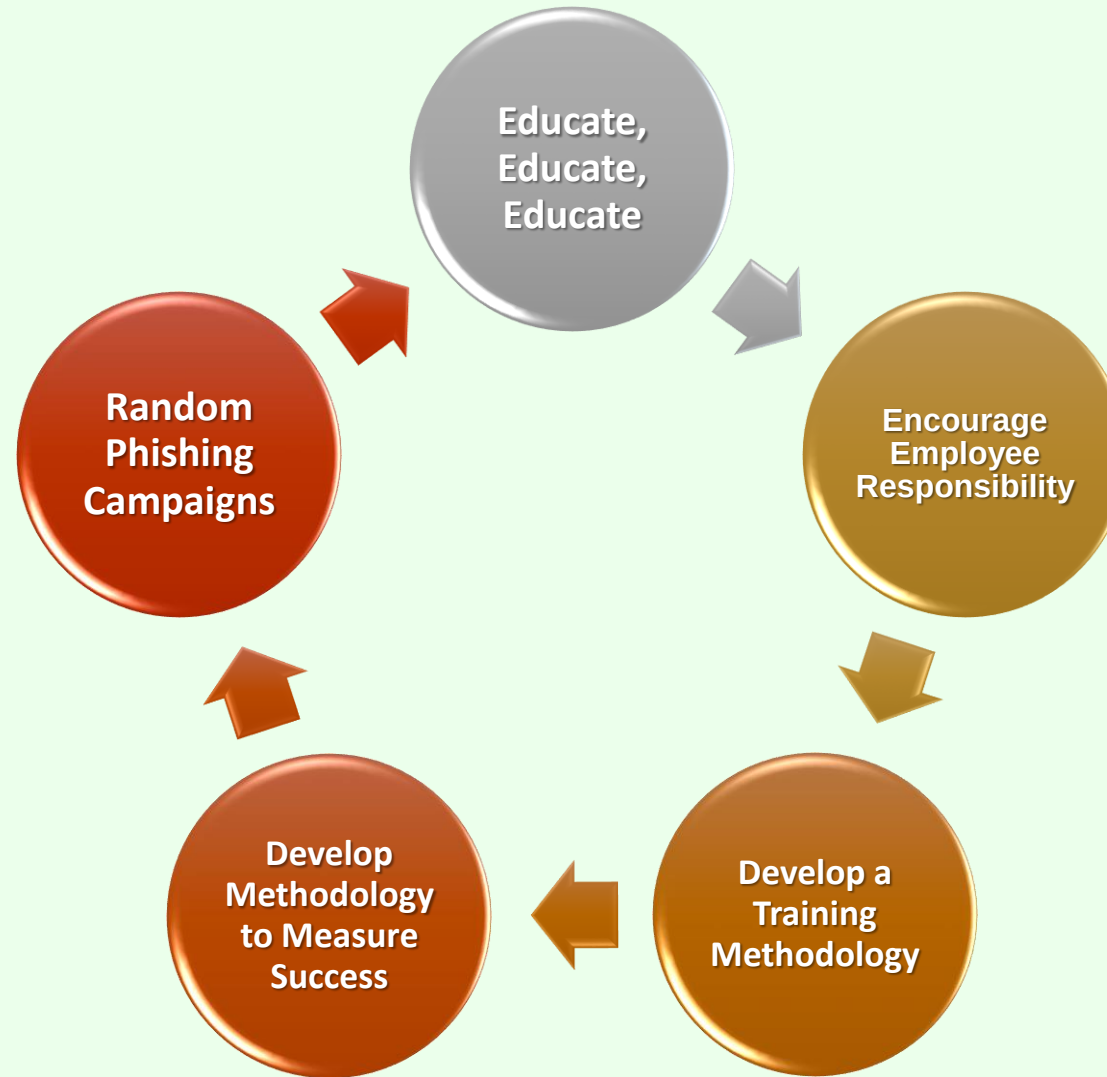
9 out of 10 phishing emails carried ransomware in March



250 percent surge in phishing



Phishing Strategy



Let's look at some true Phishing Emails



From: IT@quincyl.gov [\[mailto:IT@quincyl.gov\]](mailto:IT@quincyl.gov)

Sent: Friday, October 14, 2016 12:38 PM

Subject: [BULK] Change of Password Required Immediately

Importance: Low

We suspect a security breach happened earlier this week. In order to prevent further damage, we need everyone to change their password immediately.

Please click here to do that:

[Change Password](#)

Please do this right away. Thanks!

Sincerely,
IT

From: AccountsFacebook <ftynn@sdcf.com>

Sent: Sunday, July 9, 2017 10:31 AM

To: xxxxxx@hotmail.com

Subject: You have unread message that will be deleted in 3 days underestimating

facebook

Here's some activity you may have missed on Facebook.

[1 unread message](#)

[**Go To Facebook**](#)

[**See All Notifications**](#)

This message was sent to xxxxxx@hotmail.com. If you don't want to receive these emails from Facebook in the future, please [unsubscribe](#).

Facebook, Inc. Attention: Department 415 P.O Box 10005 Palo Alto CA 94303



**E-Payment
Transfer On Hold**

[View Accounts](#) [Privacy Promise](#) [Contact Us](#)



**USAA SECURITY
ZONE
Security
Team
USAA: 2017**

Dear USAA Member,

You have new a new e-payment deposited into your USAA account from another USAA checking account. We've temporarily put the payment on hold until you approve it.

Payments on hold will be credited into your Checking/Saving's Account within 48-72 hours after your approval. You are to update your account to approve the payment. Kindly click on the button below to update & approve your payment.

[> Approve Your
Payment](#)

USAA values your business and is committed to keeping your account and personal information safe. Thank you, USAA

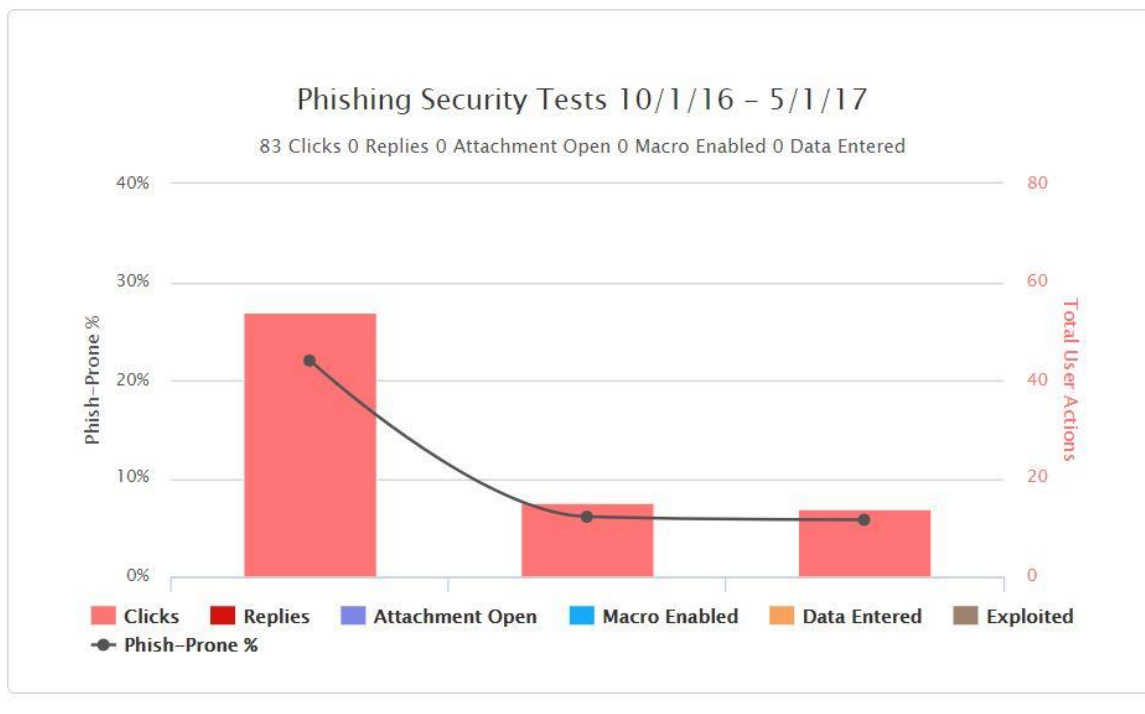


Please do not reply to this e-mail. To send a secure message to USAA,
please [contact us](#).

[Privacy Promise](#)

City of Quincy Security Awareness Training

⚙️ This Phishing Security Test	
STATUS	Closed
PHISH PRONE	22.0%
RECIPIENTS	245
FAILURES	54
CAMPAIGN END 10/20/2016 01:35 PM	



⚙️ This campaign	
STATUS	Running
LAST PHISH PRONE PERCENTAGE	4.9%
PHISHING SECURITY TESTS	2

Your payment is past due

Dear Cardholder,

The payment date for your Business Gold Rewards Card account is now passed.

Statement Balance:	\$6309.73
Payment Due:	\$6309.73

If you have already sent or scheduled your payment, please [Contact us here](#).

[Make a payment](#) [View recent activity](#) [Update alert settings](#)

Thank you for your Cardmembership.

Sincerely,
American Express Customer Service

If for any reason you want to stop receiving this alert simply [click here](#).

* Payment Due reflects the amount due on your account as of the statement close date.
Check your online statement for the most current information about your account.

Was this e-mail helpful? Please [click here](#) to give us your feedback.



For your security:



[Contact Customer Service](#) [View Our Privacy Statement](#) [Add Us to Your Address Book](#)

Your Cardmember information is included in the upper-right corner to help you recognize this as a customer service e-mail from American Express. Using the spam/junk mail function may not block servicing messages from being sent to your email account. To learn more about e-mail security or report a suspicious e-mail, please visit us at americanexpress.com/phishing. We kindly ask you not to reply to this e-mail but instead contact us securely

Each of the Hyperlinks point to the Internet link below.
No where in the hyperlink does it point to the American Express website.

<http://ens.secureconnection.moneytransaction.kb4.io/XcmVujaXBpZWh50X2lkPTVI5OTgwMcMTY0XNSZjYW1wEYWHlnbl9ydW5faWQ9Nzk0dOTQ1JmFjdGlvbj1jbG1jayZ1cmw9aHR0cHM6Ly9wYWdlcy5rbm93YmU0dHJhaW5pbmcuY29tL3BhZ2VzL2MzOTU1YjFjNDhh>



**Navigating
the Path to Leadership**

From: MyRetirement [mailto:MyRetirement@MyRetirement-investments.com]
Sent: Wednesday, July 12, 2017 1:44 PM
To: Jim Murphy
Subject: Your Statement is Available Online Now

Not personalized to the recipient
nor signed by an actual employee

Your statement is ready for your review



Dear MyRetirement Customer,

Thank you for choosing to receive your statement
through eDelivery.

Quick Links

[View Statements](#)

Your latest statement is now available for your review
on [MyRetirement.com](#).

You may also request a paper copy of your statement
at no charge by calling MyRetirement at [800-555-7777](#). Representatives are available 24 hours a day,
7 days a week.

To send a secure e-mail about your account, please
go to [MyRetirement.com/contactus](#).

Thank you for choosing MyRetirement.

Sincerely,

MyRetirement Investments

Each of the Hyperlinks point to the Internet link below.
No where in the hyperlink does it point to the a real
retirement investment website.

<http://boogeymangotcha.com/myretirementinvestments/gone.html>



From: Facebook [mailto:Facebook@facebookmail-inc.net]

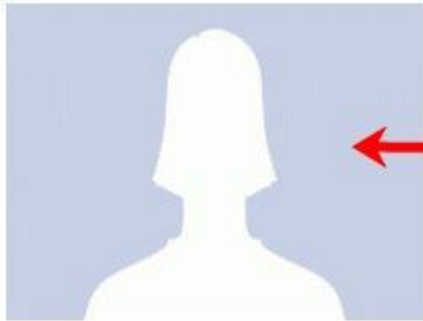
Sent: Wednesday, July 12, 2017 1:52 PM

To: Jim Murphy

Subject: Your Friend Tagged a Photo of You

← Not from Facebook Address

facebook



One of Your Friends added a photo of you.

Each of the Hyperlinks point to the Internet link below.
No where in the hyperlink does it point to the real Facebook website.

<https://facebookmail-inc.io/pages/c3955b1c48a>

See Photo

Go to Notifications

This message was sent to your email address. If you don't want to receive these emails from Facebook in the future, please click: [unsubscribe](#).

Facebook LLC, Attention: Department 415 P.O Box 90210 Columbus OH 90210

From: Pizza Hut [mailto:PizzaHutCoupons@PizzaHut.com]

Sent: Wednesday, July 12, 2017 1:50 PM

To: Jim Murphy

Subject: 55th Anniversary and Free Pizza



FREE PERSONAL PAN PIZZA!

We are celebrating our anniversary and want to celebrate with you. Enjoy a personal pan pizza on us! Click below to print your coupon.

[Get Free Pizza Coupon](#)

[Unsubscribe](#) | [Contact Us](#)

Copyright © | All rights reserved

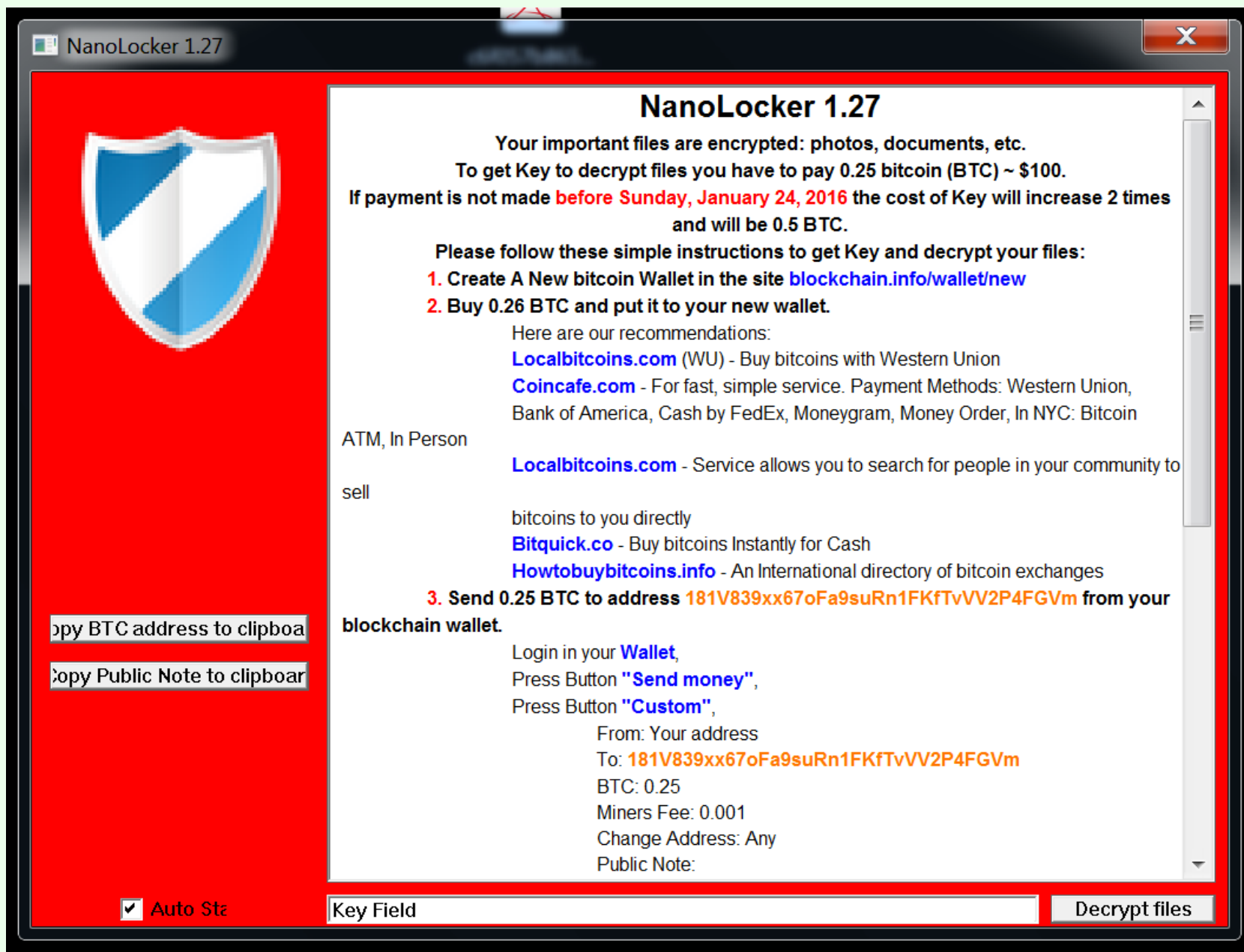
Each of the Hyperlinks point to the Internet link below. No where in the hyperlink does it point to the real Pizza Hut website. (Notice misspelling)

<https://pizahut.com/XcmVujaXBpZW50X2lkPTVI5OTgwMcMTY0XNSZjYW1wEYWHlnbl9ydW5faWQ9Nzk0dOTQ1JmFjdGlvbjljbGljayZ1cmw9aHR0cHM6Ly9wYWdlcy5rbm93YmU0dHJhaW5pbmcuY29tL3BhZ2VzL2MzOTU1YFjNDhh>



**Navigating
the Path to Leadership**





Oops! You clicked on a simulated phishing test.

Remember these three 'Rules To Stay Safe Online'

✓ **RULE NUMBER ONE:**

- Stop, Look, Think!
- Use that delete key

✓ **RULE NUMBER TWO:**

- Do I spot a Red Flag?
- Verify suspicious email with the sender via a different medium

✓ **RULE NUMBER THREE:**

- "When in doubt, throw it out". There are a thousand ways that internet criminals will try to scam you, and only one way to stay safe: Stay alert as YOU are the last line of defense!



PLEASE NOTE:

This message came from KnowBe4, Inc. and not from the company whose name is mentioned in the body of the email message, as that company has no association with KnowBe4, Inc. and does not endorse the services of KnowBe4, Inc. The purpose of this message is to demonstrate how phishing attacks can come in emails that deceptively appear to be from reputable companies.

Social Engineering Red Flags



FROM

- I don't recognize the sender's email address as someone I **ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- I **don't know the sender personally** and they **were not vouched for** by someone I trust.
- I **don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.



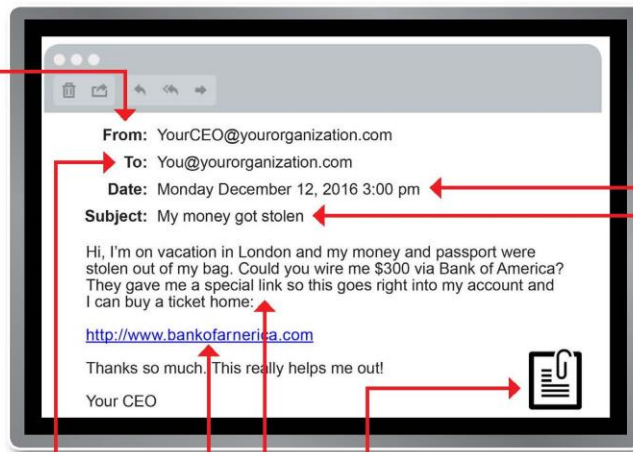
TO

- I was cc'd on an email sent to one or more people, but I **don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.



HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big red flag**.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."



DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?



SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something I **never sent or requested**?



ATTACHMENTS

- The sender included an email attachment that I **was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt file**.



CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?



<http://www.gmisillinois.org/>



**Navigating
the Path to Leadership**