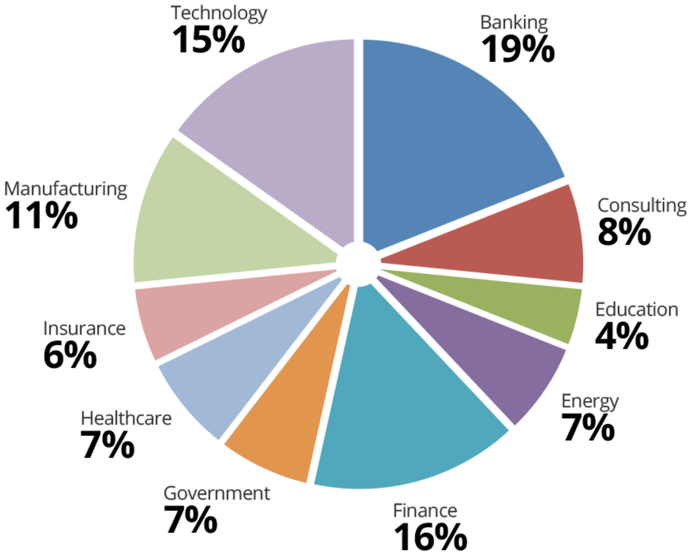
Social Media, Business Fraud, Phishing

Secrets To A Successful Security Awareness Program

Roger A. Grimes
KnowBe4
Data-Driven Defense Evangelist
e:rogerg@knowbe4.com

KnowBe4, Inc.

- The world’s most popular integrated Security Awareness Training and Simulated Phishing platform
- Based in Tampa Bay, Florida, founded in 2010
- CEO & employees are ex-antivirus, IT Security pros
- 200% growth year over year
- We help tens of thousands of organizations manage the problem of social engineering



Roger A. Grimes
Data-Driven Defense Evangelist
KnowBe4, Inc.

Twitter: @rogeragrimes
LinkedIn: www.linkedin.com/in/rogeragrimes

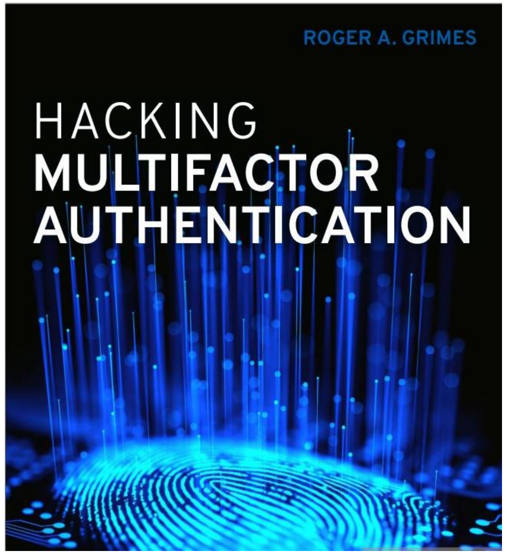
About Roger

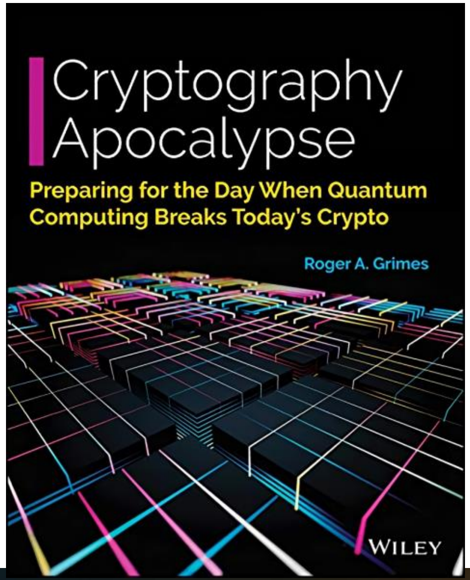
- 30 years plus in computer security
- Expertise in host and network security, IdM, crypto, PKI, APT, honeypot, cloud security
- Consultant to world's largest companies and militaries for decades
- Previous worked for Foundstone, McAfee, Microsoft
- Written 12 books and over 1,000 magazine articles
- *InfoWorld* and *CSO* weekly security columnist 2005 - 2019
- Frequently interviewed by magazines (e.g. Newsweek) and radio shows (e.g. NPR's All Things Considered)

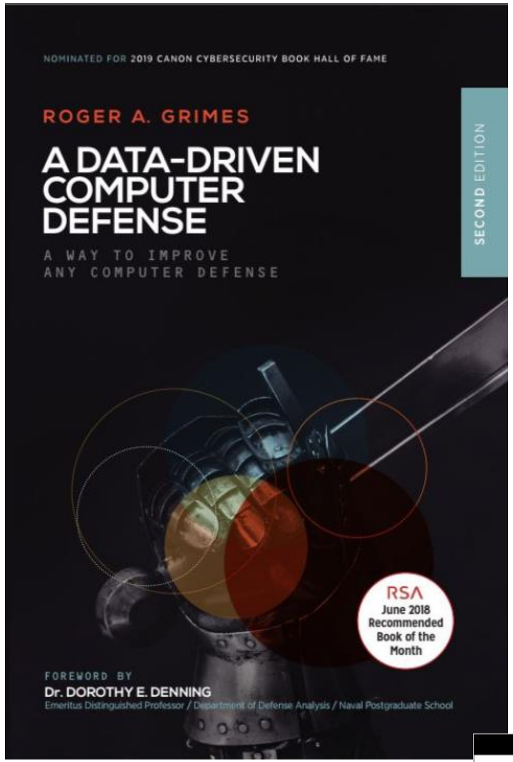
Certification exams passed include:

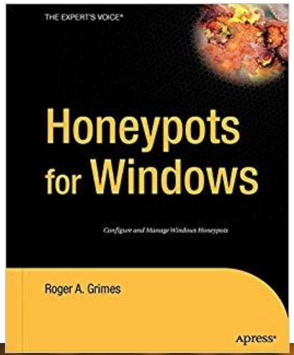
- CPA
- CISSP
- CISM, CISA
- MCSE: Security, MCP, MVP
- CEH, TISCA, Security+, CHFI
- yada, yada

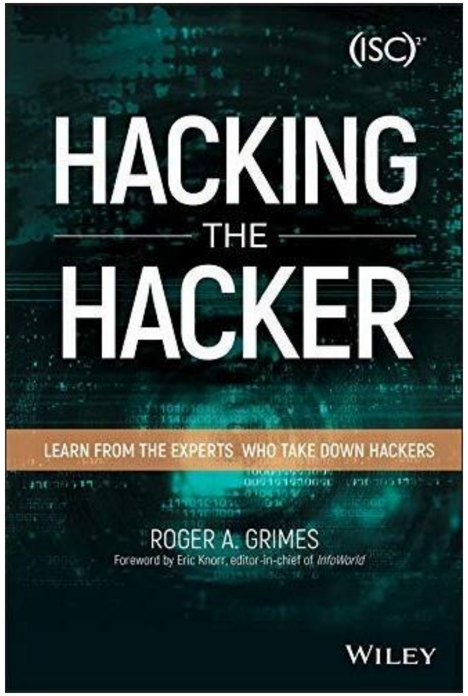
Roger's Books

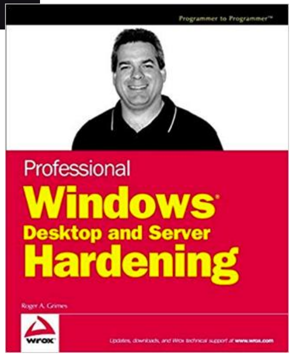


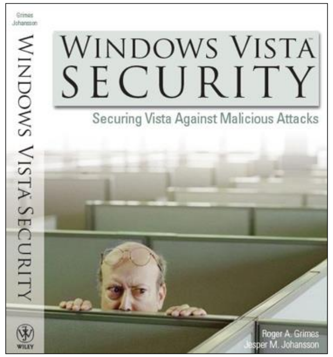

Cryptography
Apocalypse
Preparing for the Day When Quantum
Computing Breaks Today's Crypto
Roger A. Grimes
WILEY

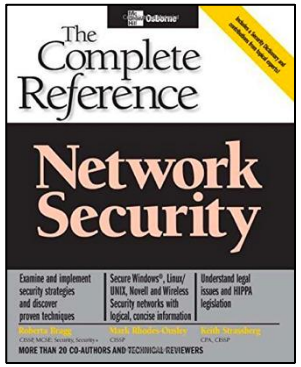


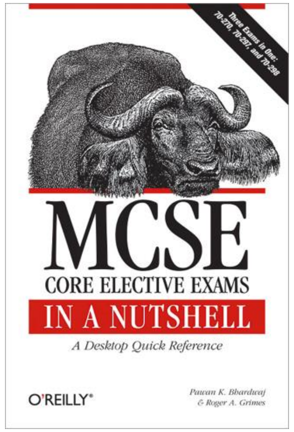


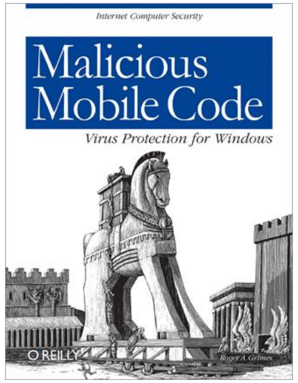

(ISC)²
HACKING
THE
HACKER
LEARN FROM THE EXPERTS WHO TAKE DOWN HACKERS
ROGER A. GRIMES
Foreword by Eric Knorr, editor-in-chief of InfoWorld
WILEY

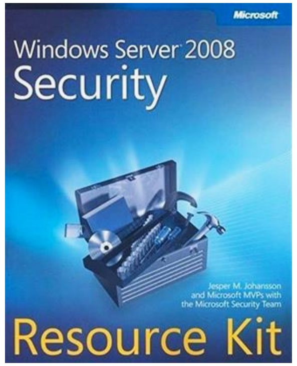












Agenda

- Phishing Examples
- Defenses

Problem – Overwhelming Numbers

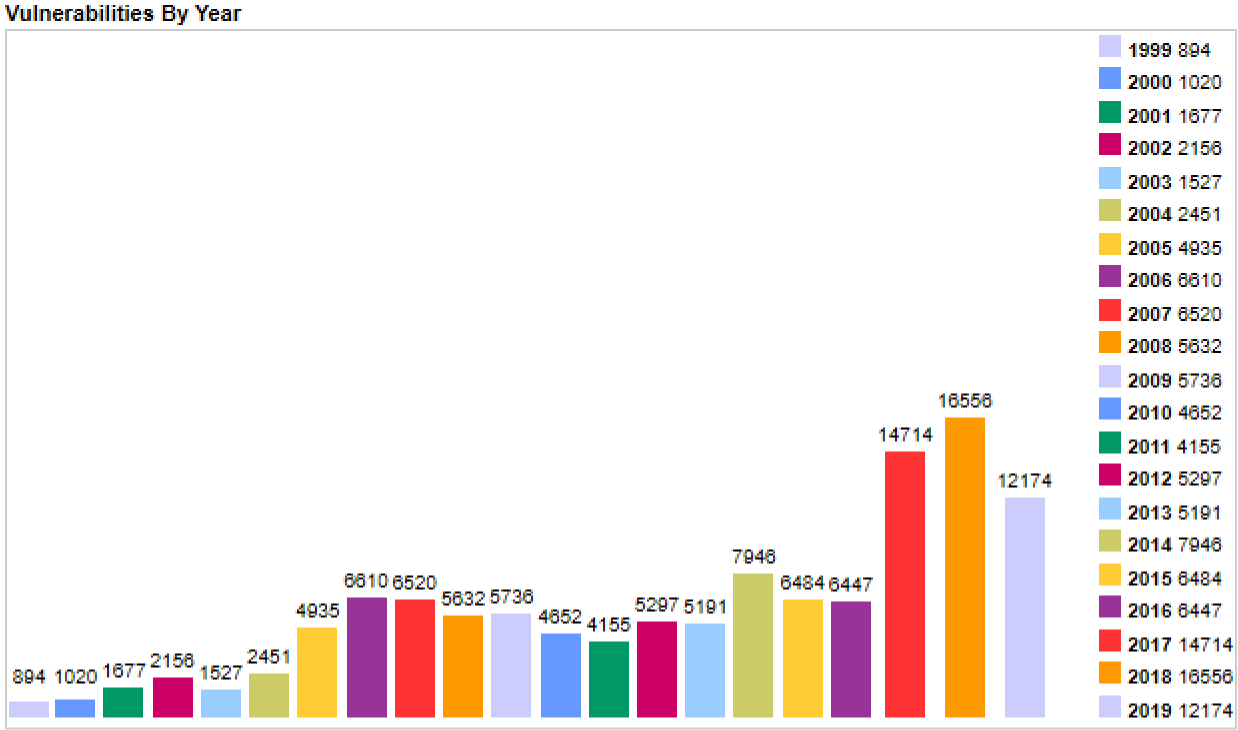
Problem Definition –

How Did It Get This Way?

And this is just (known public) vulnerabilities, doesn't include hackers and a hundred million malware programs

Sheer Number of Threats

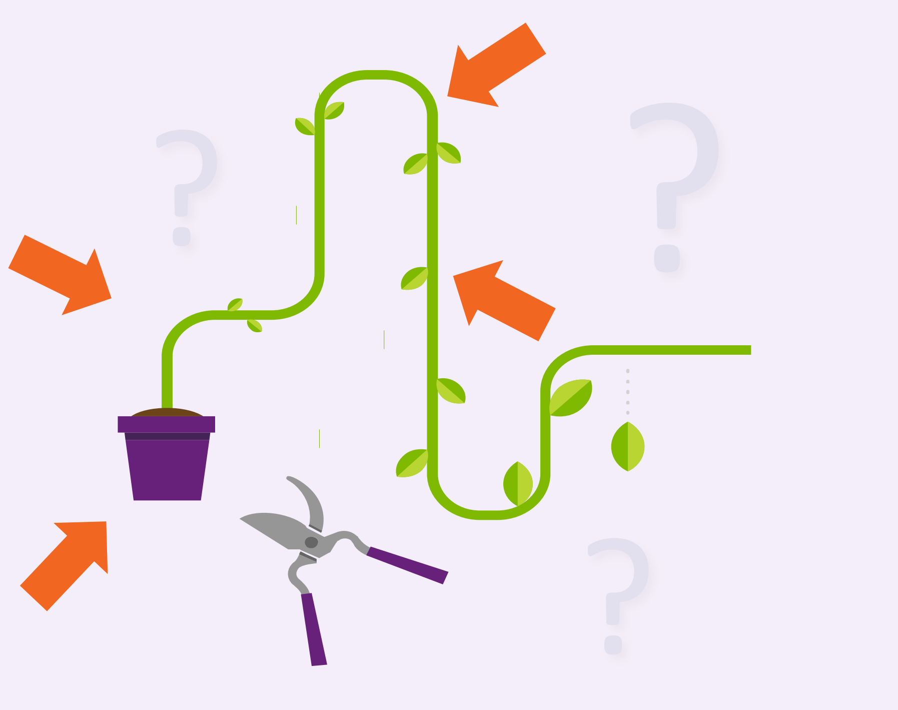
- Avg: 5K-16K+ new threats/year
- 13-45/day, day after day



How Hackers and Malware Break In

Here Are the 10 Ways:

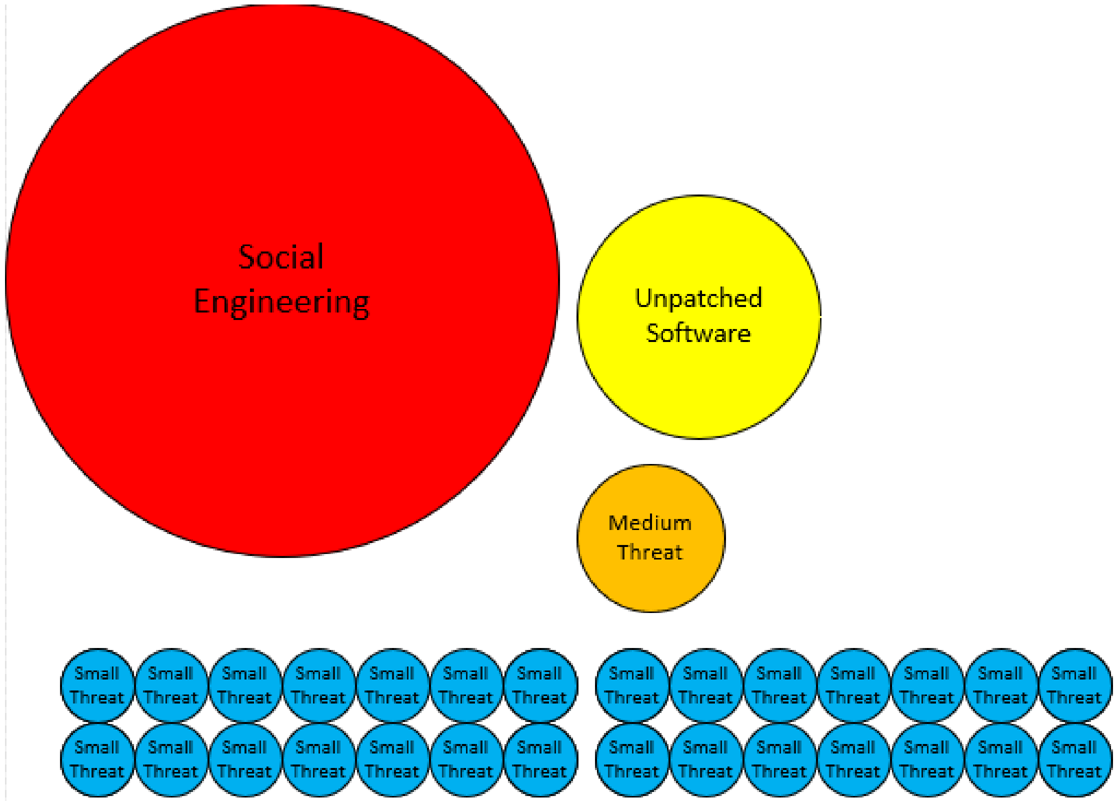
- Programming Bug
- Social Engineering
- Authentication Attack
- Human Error
- Misconfiguration
- Eavesdropping/MitM
- Data/Network Traffic Malformation
- Insider Attack
- 3rd Party Reliance Issue
- Physical Attack



Biggest Initial Breach Root Causes for Most Companies

- Social Engineering
- Unpatched Software

- But don’t trust me, measure your own risk



Social engineering is responsible for 70% - 90% of all malicious data breaches

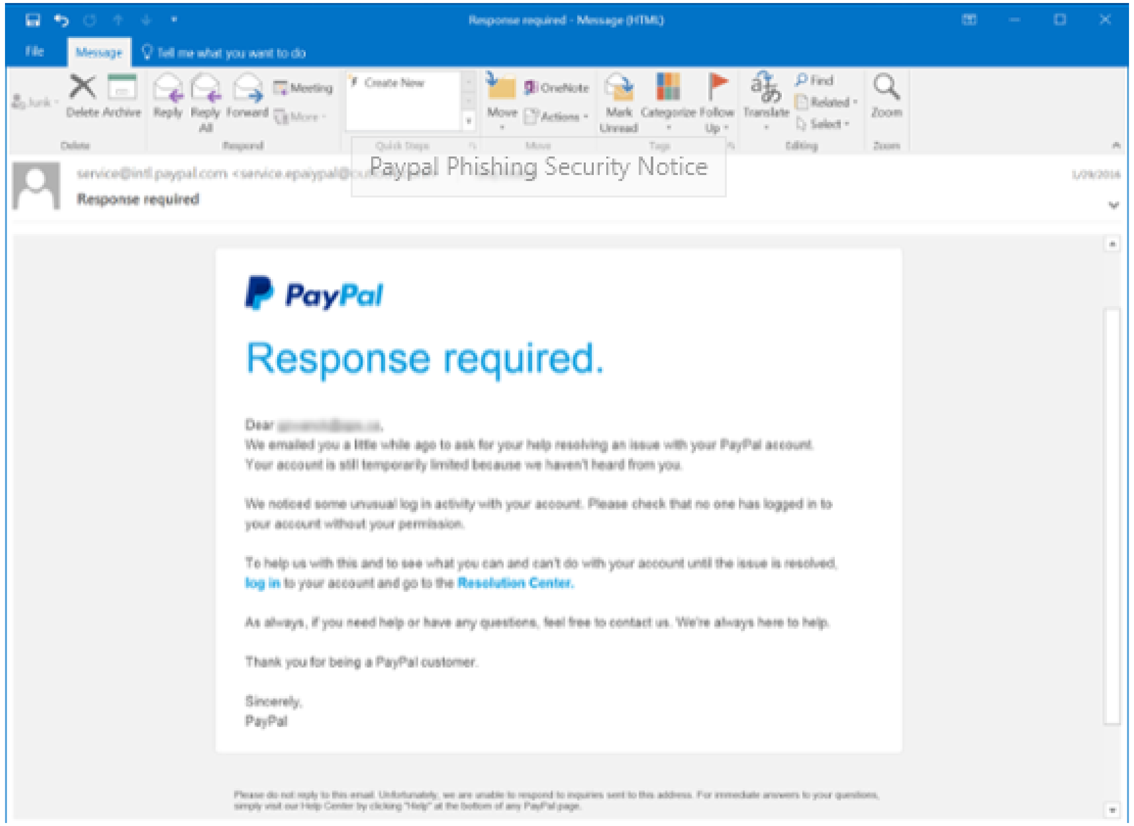
https://blog.knowbe4.com/70-to-90-of-all-malicious-breaches-are-due-to-social-engineering-and-phishing-attacks

What is Phishing?

- The process of maliciously masquerading as a trusted entity to acquire unauthorized information or to created a desired action that is contrary to the victim’s or their company’s self-interests
- Simply put - a “con”, criminal-intent
- Often done using in-person, email, IM, SMS, phone, etc.
- AKA phishing, spearphishing, spamming, vishing, etc.
- Emails/messages/SMS/Voice calls claiming to be from friends, co-workers, popular social web sites, banks, auction sites, or IT administrators are commonly used to lure the unsuspecting public.

What is Phishing?

Examples



Paypal Phishing Security Notice

service@intl.paypal.com <service.epaypal@cu...

1/29/2016

Response required

PayPal

Response required.

Dear [redacted].
We emailed you a little while ago to ask for your help resolving an issue with your PayPal account.
Your account is still temporarily limited because we haven't heard from you.

We noticed some unusual log in activity with your account. Please check that no one has logged in to your account without your permission.

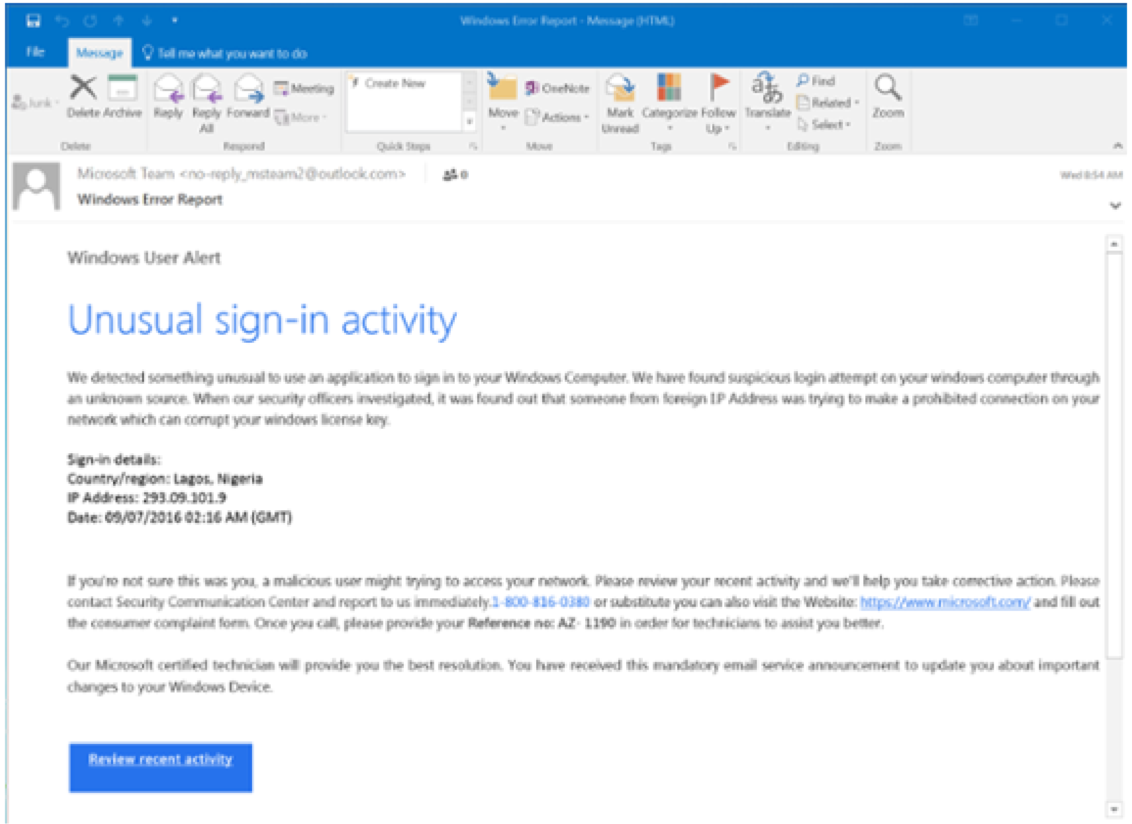
To help us with this and to see what you can and can't do with your account until the issue is resolved, **log in** to your account and go to the **Resolution Center.**

As always, if you need help or have any questions, feel free to contact us. We're always here to help.

Thank you for being a PayPal customer.

Sincerely,
PayPal

Please do not reply to this email. Unfortunately, we are unable to respond to inquiries sent to this address. For immediate answers to your questions, simply visit our Help Center by clicking "Help" at the bottom of any PayPal page.



Microsoft Team <no-reply_msteam2@outlook.com>

Wed 8:54 AM

Windows Error Report

Windows User Alert

Unusual sign-in activity

We detected something unusual to use an application to sign in to your Windows Computer. We have found suspicious login attempt on your windows computer through an unknown source. When our security officers investigated, it was found out that someone from foreign IP Address was trying to make a prohibited connection on your network which can corrupt your windows license key.

Sign-in details:
Country/region: Lagos, Nigeria
IP Address: 293.09.101.9
Date: 09/07/2016 02:16 AM (GMT)

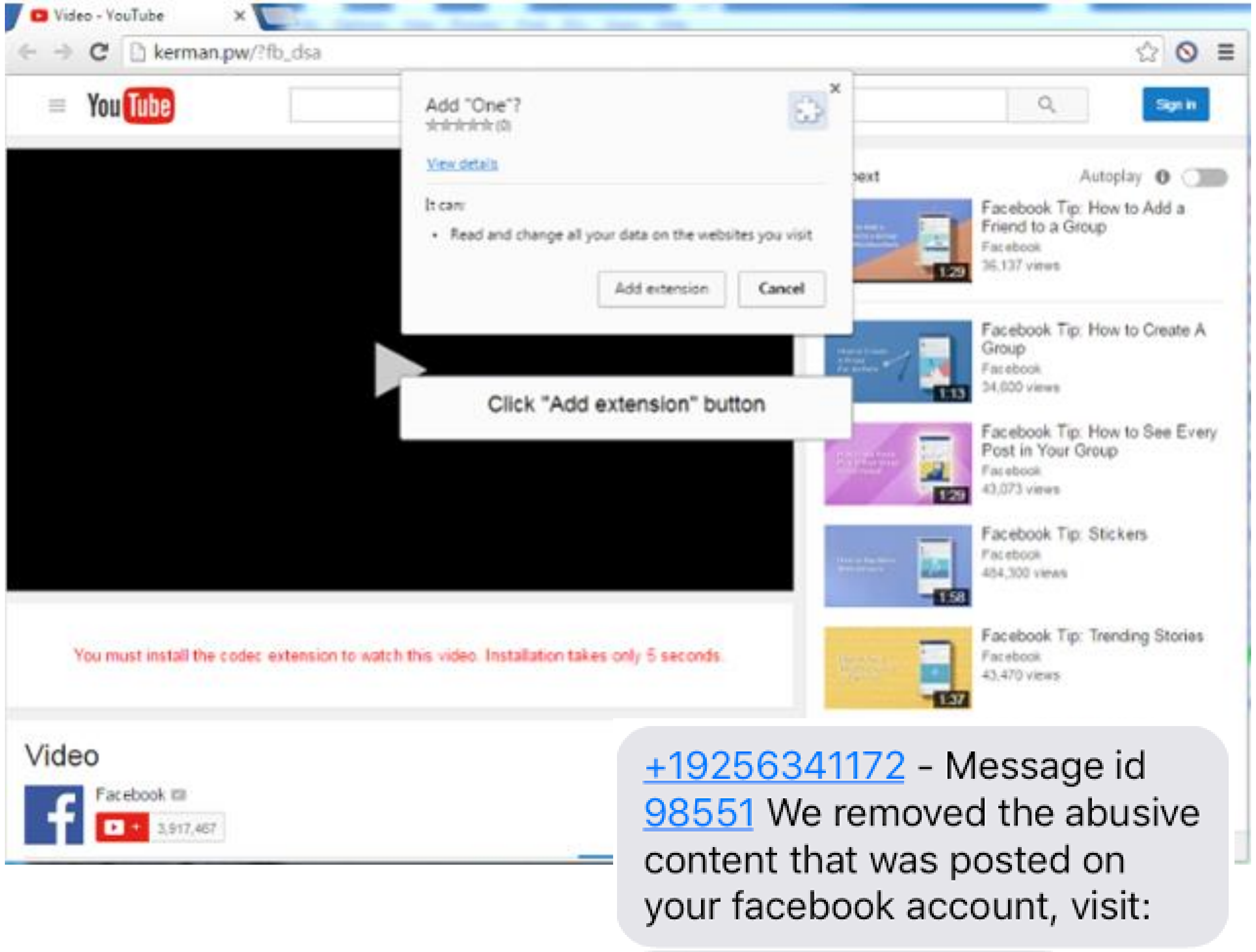
If you're not sure this was you, a malicious user might trying to access your network. Please review your recent activity and we'll help you take corrective action. Please contact Security Communication Center and report to us immediately.1-800-816-0380 or substitute you can also visit the Website: https://www.microsoft.com/ and fill out the consumer complaint form. Once you call, please provide your **Reference no: AZ- 1190** in order for technicians to assist you better.

Our Microsoft certified technician will provide you the best resolution. You have received this mandatory email service announcement to update you about important changes to your Windows Device.

Review recent activity

What is Phishing?

Examples



Add "One"?

View details

It can:

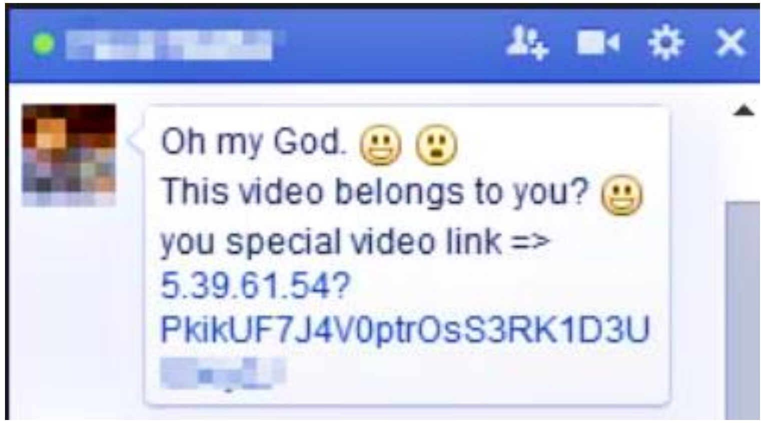
- Read and change all your data on the websites you visit

Add extension | Cancel

Click "Add extension" button

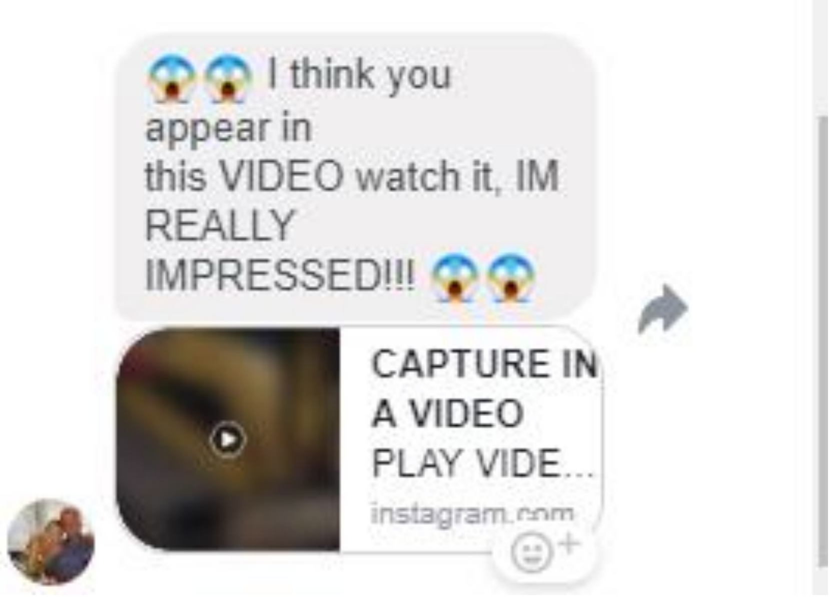
You must install the codec extension to watch this video. Installation takes only 5 seconds.

+19256341172 - Message id 98551 We removed the abusive content that was posted on your facebook account, visit:



[redacted]

Oh my God. 😃 😮
This video belongs to you? 😃
you special video link =>
5.39.61.54?
PkikUF7J4V0ptrOsS3RK1D3U
[redacted]

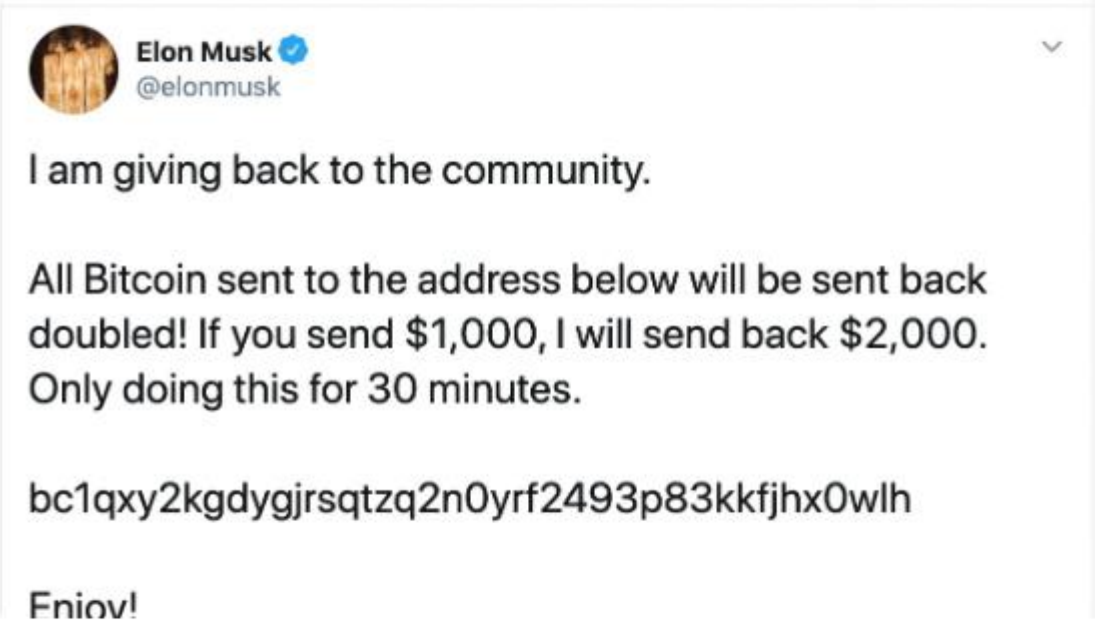


😱😱 I think you appear in
this VIDEO watch it, IM REALLY IMPRESSED!!! 😱😱

CAPTURE IN A VIDEO
PLAY VIDE...
instagram.com

What is Phishing?

Twitter Example



Elon Musk
@elonmusk

I am giving back to the community.

All Bitcoin sent to the address below will be sent back doubled! If you send $1,000, I will send back $2,000. Only doing this for 30 minutes.

bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh

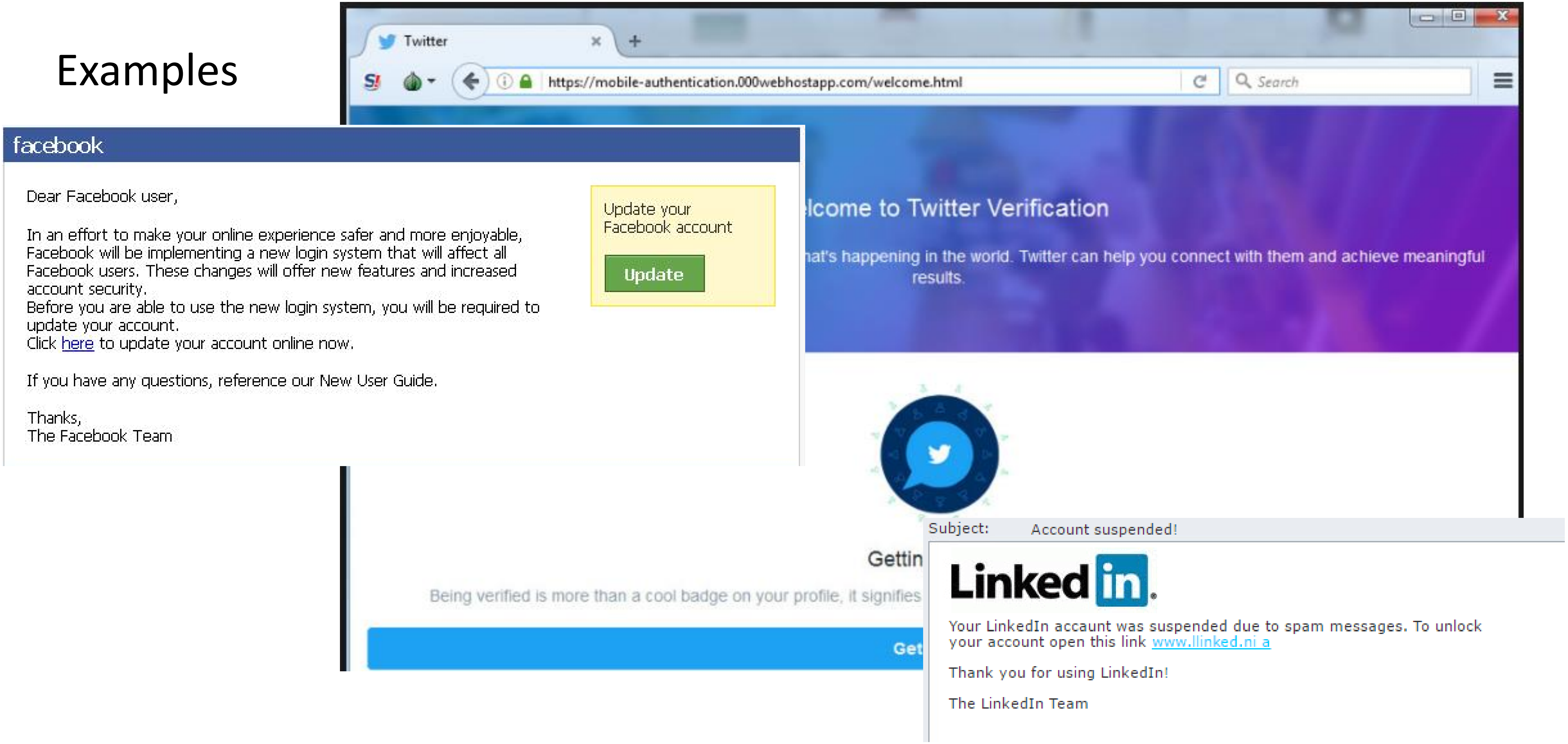
Enjoy!

Bezos, Musk, Gates, Obama and others target of cryptocurrency hack on Twitter

www.usatoday.com

What is Phishing?

Examples



Twitter
https://mobile-authentication.000webhostapp.com/welcome.html
Search

lcome to Twitter Verification

hat's happening in the world. Twitter can help you connect with them and achieve meaningful results.

Gettin

Being verified is more than a cool badge on your profile, it signifies

Dear Facebook user,

In an effort to make your online experience safer and more enjoyable, Facebook will be implementing a new login system that will affect all Facebook users. These changes will offer new features and increased account security.
Before you are able to use the new login system, you will be required to update your account.
Click here to update your account online now.

If you have any questions, reference our New User Guide.

Thanks,
The Facebook Team

Update your Facebook account

Subject: Account suspended!

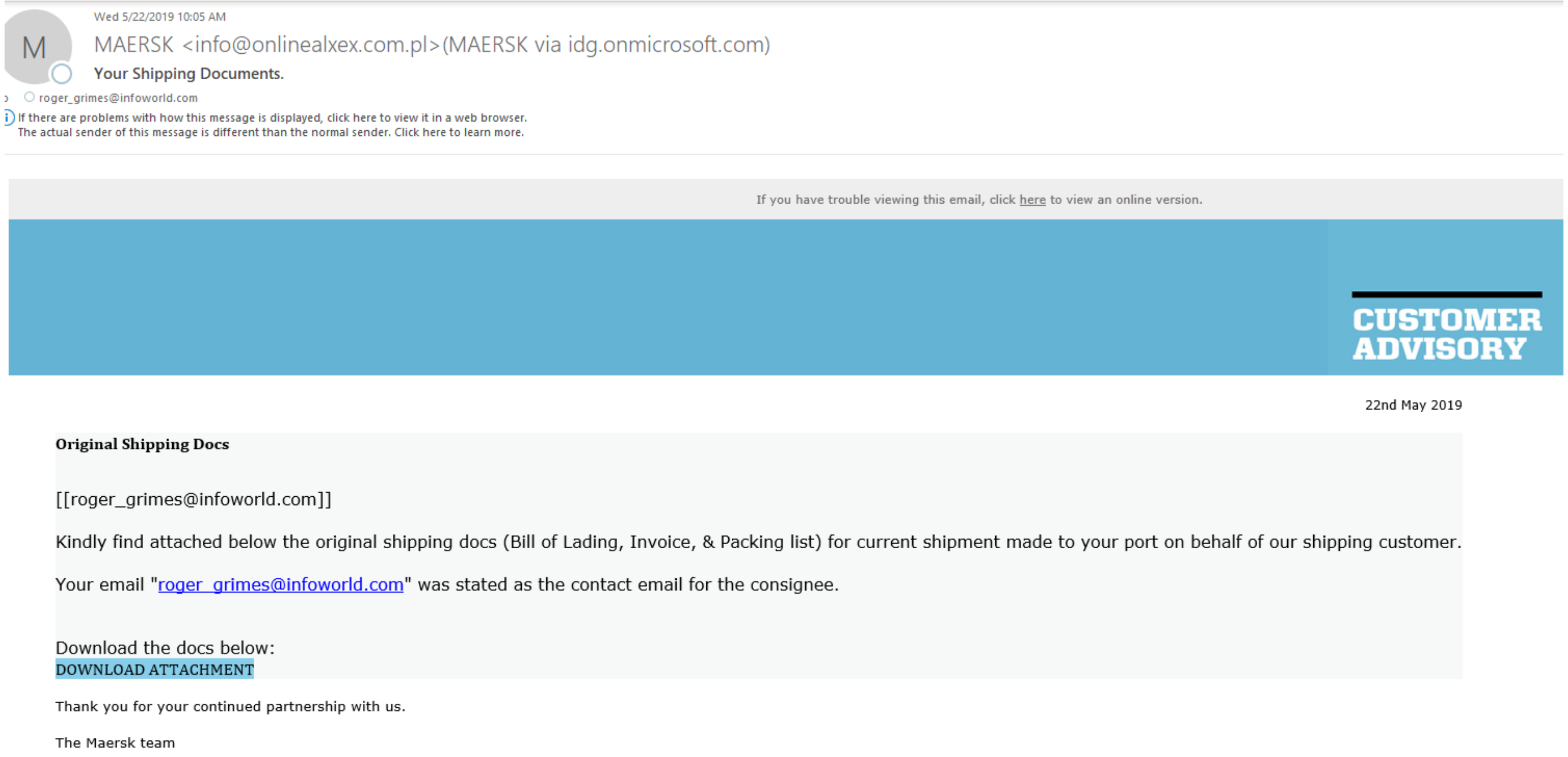
Your LinkedIn accaunt was suspended due to spam messages. To unlock your account open this link www.llinked.ni a

Thank you for using LinkedIn!

The LinkedIn Team

What is Phishing?

Fake Invoice Example



Wed 5/22/2019 10:05 AM

MAERSK <info@onlinealxex.com.pl>(MAERSK via idg.onmicrosoft.com)

Your Shipping Documents.

○ roger_grimes@infoworld.com

If there are problems with how this message is displayed, click here to view it in a web browser.
The actual sender of this message is different than the normal sender. Click here to learn more.

If you have trouble viewing this email, click here to view an online version.

22nd May 2019

Original Shipping Docs

[[roger_grimes@infoworld.com]]

Kindly find attached below the original shipping docs (Bill of Lading, Invoice, & Packing list) for current shipment made to your port on behalf of our shipping customer.

Your email "roger_grimes@infoworld.com" was stated as the contact email for the consignee.

Download the docs below:
DOWNLOAD ATTACHMENT

Thank you for your continued partnership with us.

The Maersk team

Nuclear Ransomware

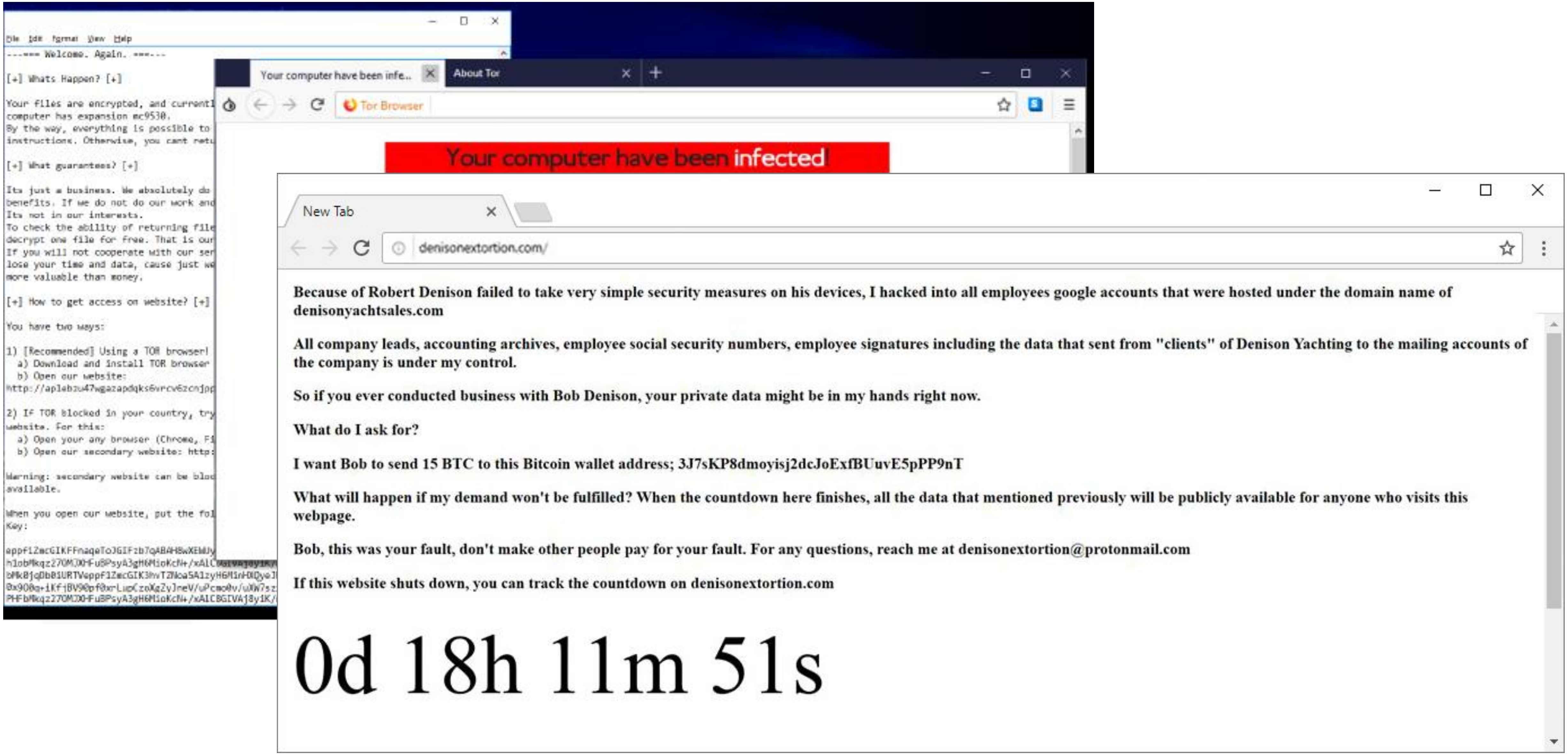
Doesn’t Just Encrypt Your Files Anymore

- Steals Intellectual Property/Data
- Steals Credentials
- Threatens Victim’s Employees and Customers
- Uses Your Stolen Data to Spear Phish Partners and Customers
- Public Shames you

Good luck having a good backup save you!

https://info.knowbe4.com/nuclear-ransomware

Ransomware Examples



File Edit Format View Help
Your computer have been infe...
About Tor
Tor Browser
Your computer have been infected!
New Tab
denisonextortion.com/

```
---=== Welcome. Again. ===---

[+] Whats Happen? [+]

Your files are encrypted, and currentl
computer has expansion mc9530.
By the way, everything is possible to
instructions. Otherwise, you cant retu

[+] What guarantees? [+]

Its just a business. We absolutely do
benefits. If we do not do our work and
Its not in our interests.
To check the ability of returning file
decrypt one file for free. That is our
If you will not cooperate with our ser
lose your time and data, cause just we
more valuable than money.

[+] How to get access on website? [+]

You have two ways:

1) [Recommended] Using a TOR browser!
  a) Download and install TOR browser
  b) Open our website:
http://aplebzu47wgazapdqks6vrcv6zcnjpp

2) If TOR blocked in your country, try
website. For this:
  a) Open your any browser (Chrome, Fi
  b) Open our secondary website: http:

Warning: secondary website can be bloc
available.

When you open our website, put the fol
Key:

eppf1ZmcGIKFFnaqeToJGIFzb7qABAH8wXEWJy
h1obMkqz27OMJXHFuBPsyA3gH6MioKcN+/xAlC
bMk8jqDbB1URTVeppf1ZmcGIK3hwT2NoaSA1zyH6M1nHXQyeJ
0x9O0q+iKfjBV90pf0xrLupCzoXgZyJneV/uPcmo0v/uXW7sz
PHFbMkqz27OMJXHFuBPsyA3gH6MioKcN+/xAlCBGIVAj8y1K/
```

Because of Robert Denison failed to take very simple security measures on his devices, I hacked into all employees google accounts that were hosted under the domain name of denisonyachtsales.com

All company leads, accounting archives, employee social security numbers, employee signatures including the data that sent from "clients" of Denison Yachting to the mailing accounts of the company is under my control.

So if you ever conducted business with Bob Denison, your private data might be in my hands right now.

What do I ask for?

I want Bob to send 15 BTC to this Bitcoin wallet address; 3J7sKP8dmoyisj2dcJoExfBUuvE5pPP9nT

What will happen if my demand won't be fulfilled? When the countdown here finishes, all the data that mentioned previously will be publicly available for anyone who visits this webpage.

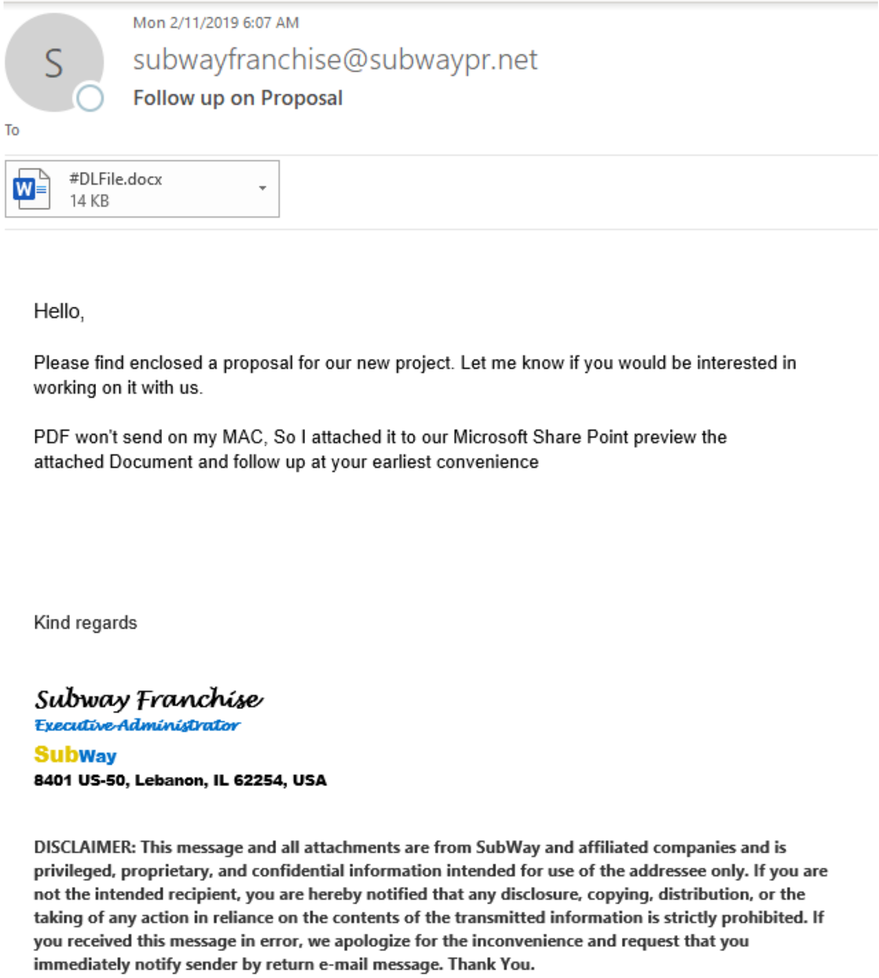
Bob, this was your fault, don't make other people pay for your fault. For any questions, reach me at denisonextortion@protonmail.com

If this website shuts down, you can track the countdown on denisonextortion.com

0d 18h 11m 51s

What is Phishing?

Fake Franchise Agreement



Mon 2/11/2019 6:07 AM

subwayfranchise@subwaypr.net

Follow up on Proposal

To

#DLFile.docx
14 KB

Hello,

Please find enclosed a proposal for our new project. Let me know if you would be interested in working on it with us.

PDF won't send on my MAC, So I attached it to our Microsoft Share Point preview the attached Document and follow up at your earliest convenience

Kind regards

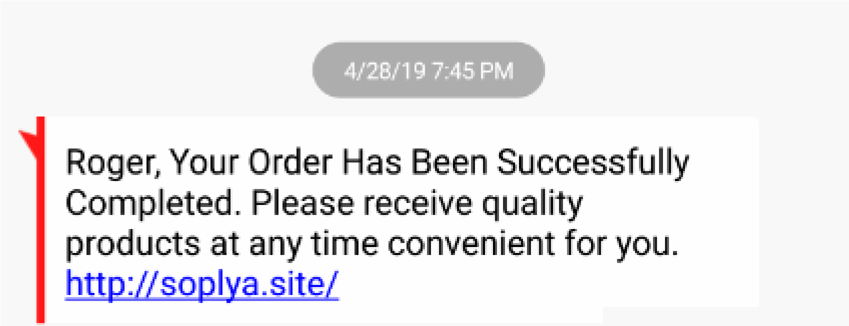
Subway Franchise
Executive Administrator
SubWay
8401 US-50, Lebanon, IL 62254, USA

DISCLAIMER: This message and all attachments are from SubWay and affiliated companies and is privileged, proprietary, and confidential information intended for use of the addressee only. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution, or the taking of any action in reliance on the contents of the transmitted information is strictly prohibited. If you received this message in error, we apologize for the inconvenience and request that you immediately notify sender by return e-mail message. Thank You.

What is Smishing?

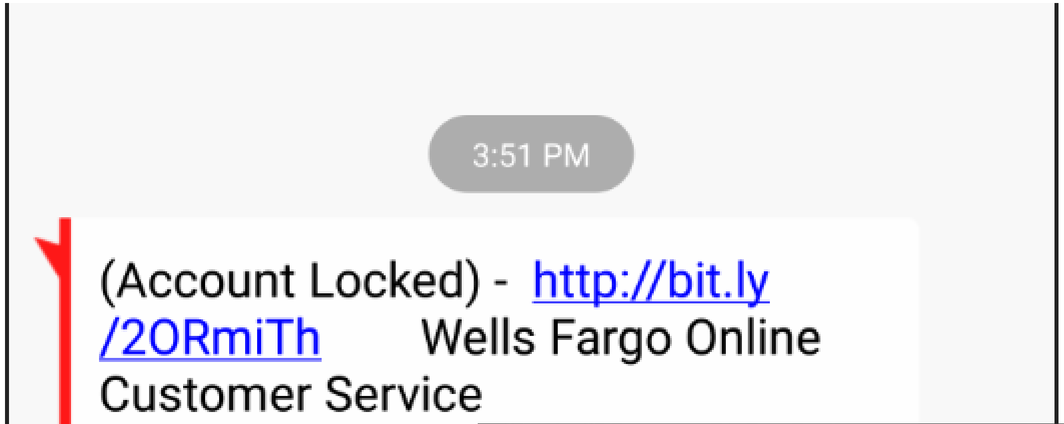
Smishing Examples

- Malicious SMS message
- Becoming very common



4/28/19 7:45 PM

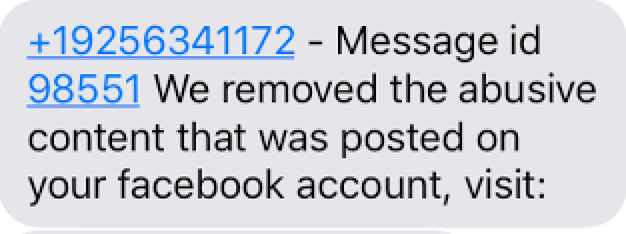
Roger, Your Order Has Been Successfully Completed. Please receive quality products at any time convenient for you. http://soplya.site/



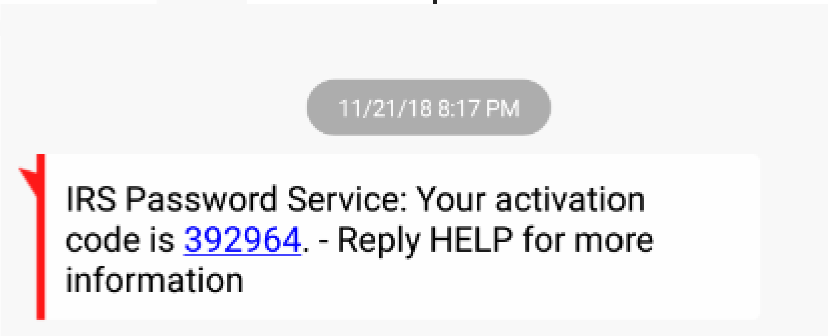
3:51 PM

(Account Locked) - http://bit.ly/2ORmiTh Wells Fargo Online Customer Service

Type a messag

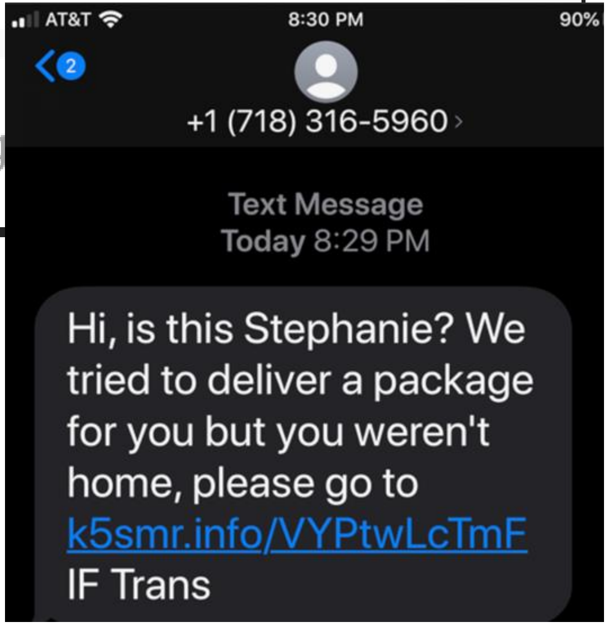


+19256341172 - Message id 98551 We removed the abusive content that was posted on your facebook account, visit:



11/21/18 8:17 PM

IRS Password Service: Your activation code is 392964. - Reply HELP for more information



+1 (718) 316-5960

Text Message
Today 8:29 PM

Hi, is this Stephanie? We tried to deliver a package for you but you weren't home, please go to k5smr.info/VYPtwLcTmF IF Trans

What is Vishing?

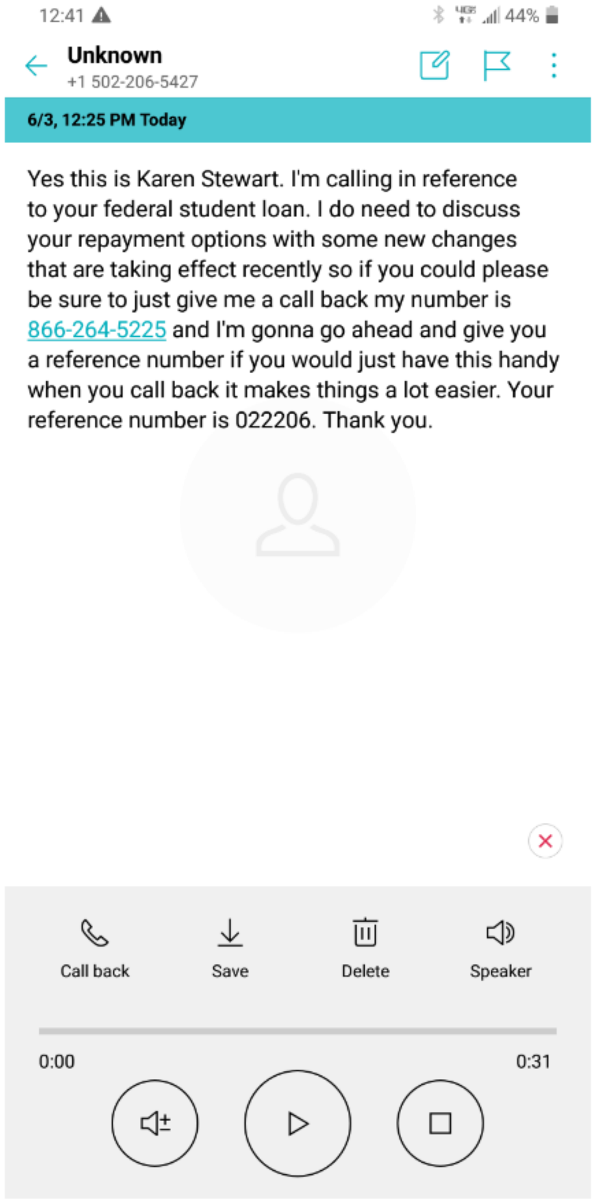
Voice Phone Phishing

- Malicious person calls pretending to be from a trusted company
- Ex: Microsoft Tech Support has detected a virus on your computer
- Ex: Paypal person claims they have detected fraud on your account and need your help to stop quickly stop it
- Often has relevant, correct information about you and your legitimate related account
- Malicious person is often using your help to break into your PC or real account, as you’re helping them over the phone

What is Vishing?

<u>Voice Phone Phishing</u>

- Malicious person calls pretending to be from a trusted company
- Becoming much more common



6/3, 12:25 PM Today

Yes this is Karen Stewart. I'm calling in reference to your federal student loan. I do need to discuss your repayment options with some new changes that are taking effect recently so if you could please be sure to just give me a call back my number is 866-264-5225 and I'm gonna go ahead and give you a reference number if you would just have this handy when you call back it makes things a lot easier. Your reference number is 022206. Thank you.

Agenda

- Phishing Examples
- Defenses

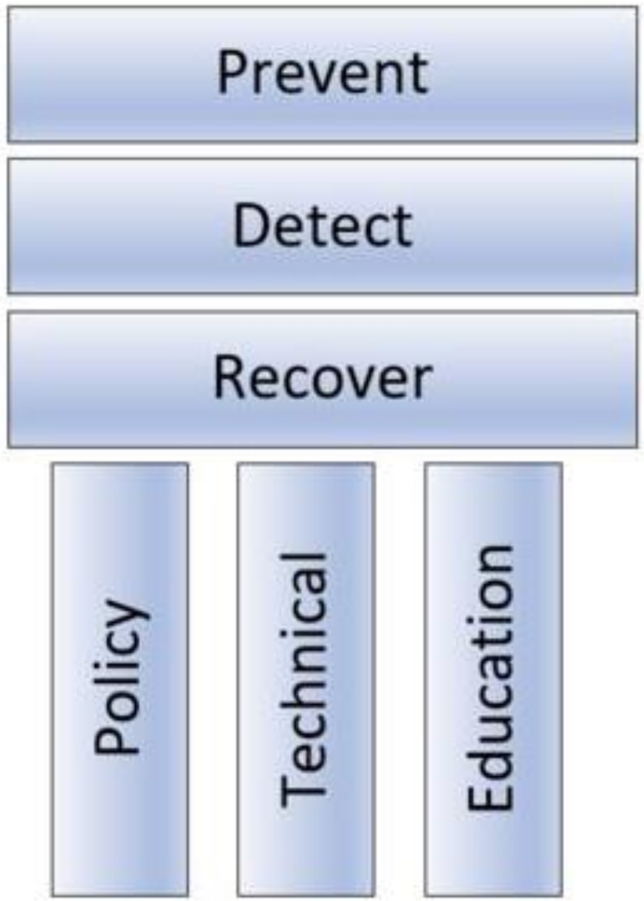
Phishing Cannot Be Beat by Intelligence

- Anyone can fall victim to social engineering
- “Smart people” are just as likely to fall victim to phishing as anyone else
- Scammers use “stressors” to make people bypass their normal skepticism survival skills
- Whether or not someone clicks on a “phish” or falls victim to a fake phone call, has more to due with awareness of digital crime than anything else
- Once people are aware of social engineering, phishing, and all it’s forms, the less likely they are to fall victim to it

Defending Against Phishing

General Defense Methods

- Policies
- Technical Controls
  - Anti-Malware Software
  - Anti-Spam/Phishing
  - Content Filtering
- Security Awareness Training



https://blog.knowbe4.com/the-three-pillars-of-the-three-computer-security-pillars

Organizational Defenses

Ultimate Phishing Guide webinar - https://info.knowbe4.com/webinar-stay-out-of-the-net

- **Defense-in-Depth**
- **Anything you can do to stop social engineering and better patch software**
- **Content Filtering**
- **Anti-Spam, Anti-Phish**
- **Email Defenses (e.g. block rogue file attachments, reputation checking, etc.)**
- **SPF, DKIM, DMARC - https://info.knowbe4.com/dmarc-spf-dkim-webinar**
- **Anti-Malware**
- **Use MFA - https://info.knowbe4.com/webinar-12-ways-to-defeat-mfa**
- **Get Cybersecurity insurance**

Best Defenses

<u>Top 5 Defenses for Most Organizations</u>

(in order of importance)

- **Mitigate Social Engineering**
- **Patch Internet-accessible software**
- **Use non-guessable passwords/multi-factor authenticati**on
  - Different passwords for every website and service
- **Teach Users How to Spot Rogue URLs**
  - https://blog.knowbe4.com/top-12-most-common-rogue-url-tricks
  - https://info.knowbe4.com/rogue-urls
- **Least-Permissive Permissions**

What Is the Goal of Security Awareness Training?

The overall goal is to help users make smarter security decisions every day

- To reach this goal you must make security awareness an integral part of your organizational culture that simply becomes reflexive

Training users to know

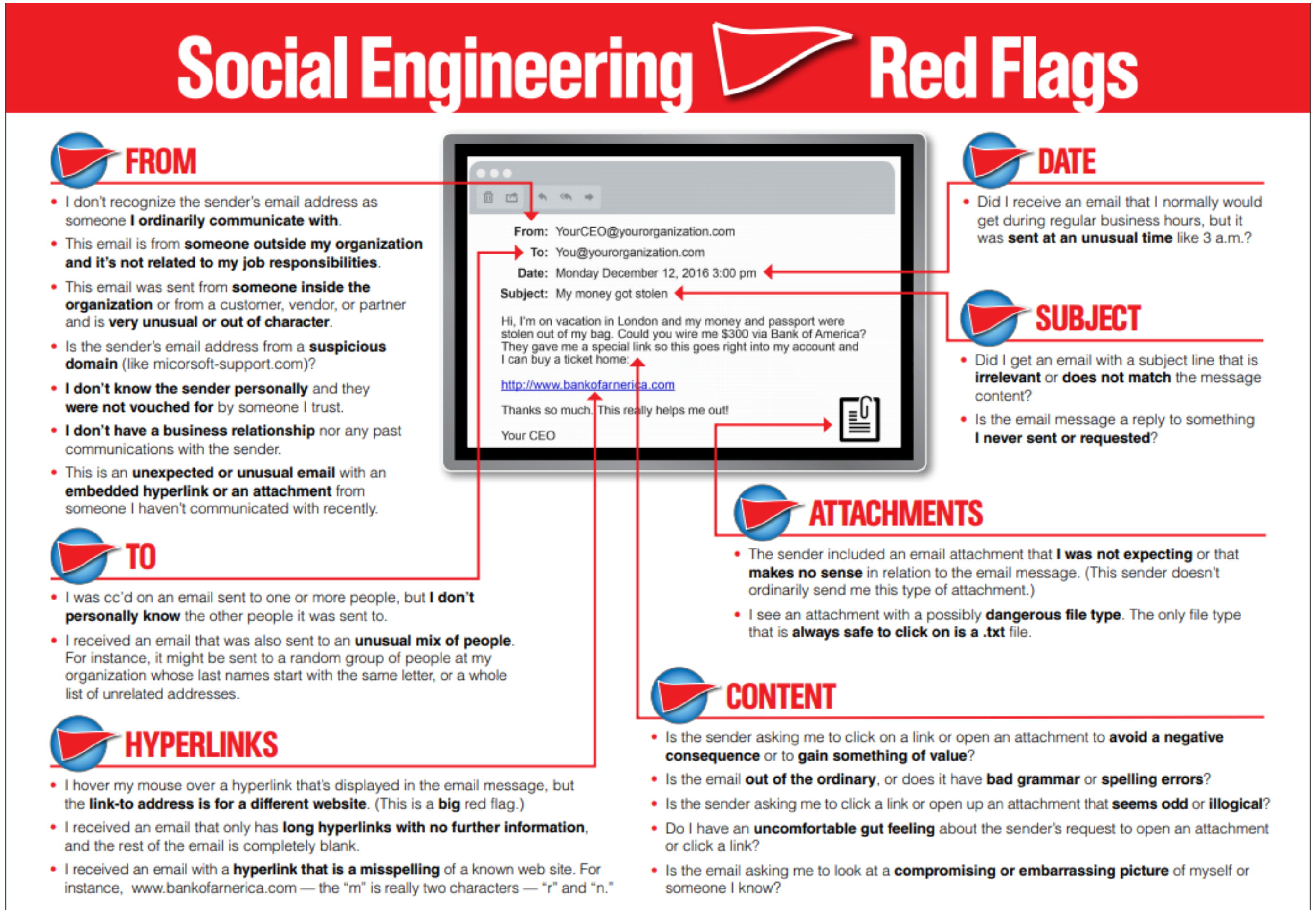
- How to spot bad things
- How to respond

Personal Defenses

General Personal Defenses

- **Security Awareness Training**
  - Phish Your Employees – monthly or more
  - Training – monthly or more
- **Hover over EVERY URL link and verify before clicking on**
  - Fighting Rogue URL Tricks webinar - https://www.knowbe4.com/webinar-library
- **When in doubt, chicken out**, let someone more knowledgeable investigate
- **You investigate** - https://info.knowbe4.com/phishing-forensics

Give “Red Flags” Training



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.”

From: YourCEO@yourorganization.com
To: You@yourorganization.com
Date: Monday December 12, 2016 3:00 pm
Subject: My money got stolen

Hi, I’m on vacation in London and my money and passport were stolen out of my bag. Could you wire me $300 via Bank of America? They gave me a special link so this goes right into my account and I can buy a ticket home:

http://www.bankofarnerica.com

Thanks so much. This really helps me out!

Your CEO

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**?

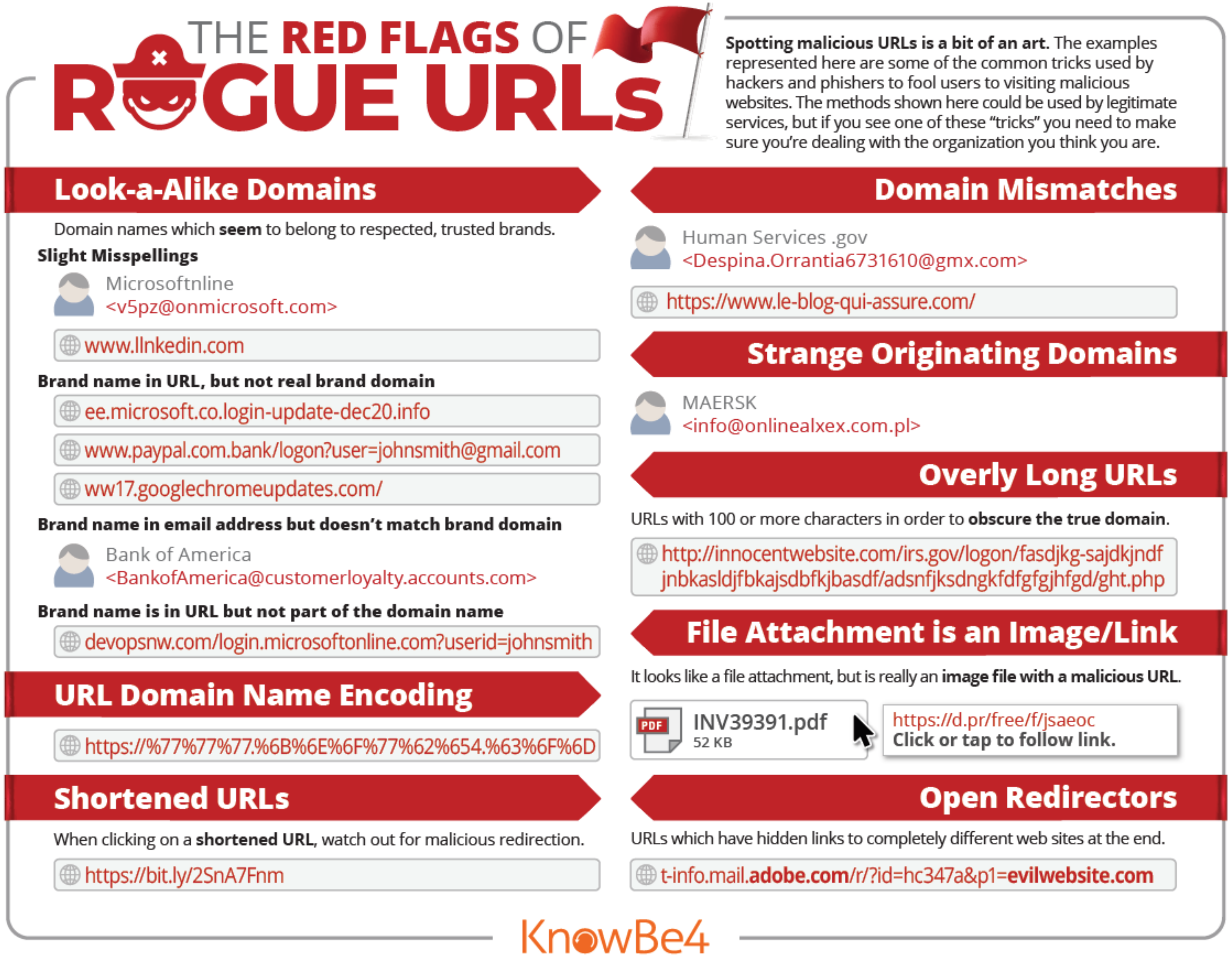
ATTACHMENTS

- 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?

https://blog.knowbe4.com/share-the-red-flags-of-social-engineering-infographic-with-your-employees



THE RED FLAGS OF ROGUE URLs

Spotting malicious URLs is a bit of an art. The examples represented here are some of the common tricks used by hackers and phishers to fool users to visiting malicious websites. The methods shown here could be used by legitimate services, but if you see one of these “tricks” you need to make sure you’re dealing with the organization you think you are.

Look-a-Alike Domains

Domain names which **seem** to belong to respected, trusted brands.

Slight Misspellings

Microsoftnline
<v5pz@onmicrosoft.com>

www.lInkedin.com

Brand name in URL, but not real brand domain

ee.microsoft.co.login-update-dec20.info

www.paypal.com.bank/logon?user=johnsmith@gmail.com

ww17.googlechromeupdates.com/

Brand name in email address but doesn’t match brand domain

Bank of America
<BankofAmerica@customerloyalty.accounts.com>

Brand name is in URL but not part of the domain name

devopsnw.com/login.microsoftonline.com?userid=johnsmith

URL Domain Name Encoding

https://%77%77%77.%6B%6E%6F%77%62%654.%63%6F%6D

Shortened URLs

When clicking on a **shortened URL**, watch out for malicious redirection.

https://bit.ly/2SnA7Fnm

Domain Mismatches

Human Services .gov
<Despina.Orrantia6731610@gmx.com>

https://www.le-blog-qui-assure.com/

Strange Originating Domains

MAERSK
<info@onlinealxex.com.pl>

Overly Long URLs

URLs with 100 or more characters in order to **obscure the true domain.**

http://innocentwebsite.com/irs.gov/logon/fasdjkg-sajdkjndf jnbkasldjfbkajsdbfkjbasdf/adsnfjksdngkfdfgfgjhfgd/ght.php

File Attachment is an Image/Link

It looks like a file attachment, but is really an **image file with a malicious URL.**

PDF INV39391.pdf
52 KB

https://d.pr/free/f/jsaeoc
Click or tap to follow link.

Open Redirectors

URLs which have hidden links to completely different web sites at the end.

t-info.mail.**adobe.com**/r/?id=hc347a&p1=**evilwebsite.com**

KnowBe4

https://blog.knowbe4.com/top-12-most-common-rogue-url-tricks

The KnowBe4 Security Awareness Program WORKS

Baseline Testing

Use simulated phishing to baseline assess the Phish-prone™ percentage of your users.

Train Your Users

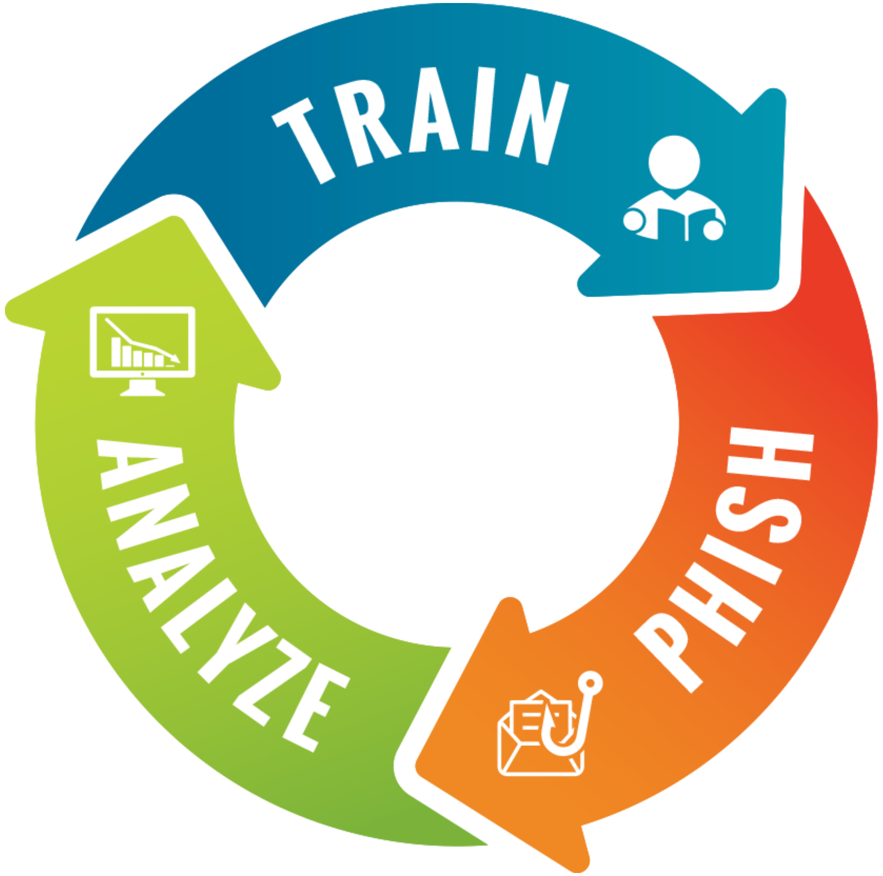
The world's largest library of security awareness training content; including interactive modules, videos, games, posters and newsletters. Automated training campaigns with scheduled reminder emails.

Phish Your Users

Best-in-class, fully automated simulated phishing attacks, hundreds of templates with unlimited usage, and community phishing templates.

See the Results

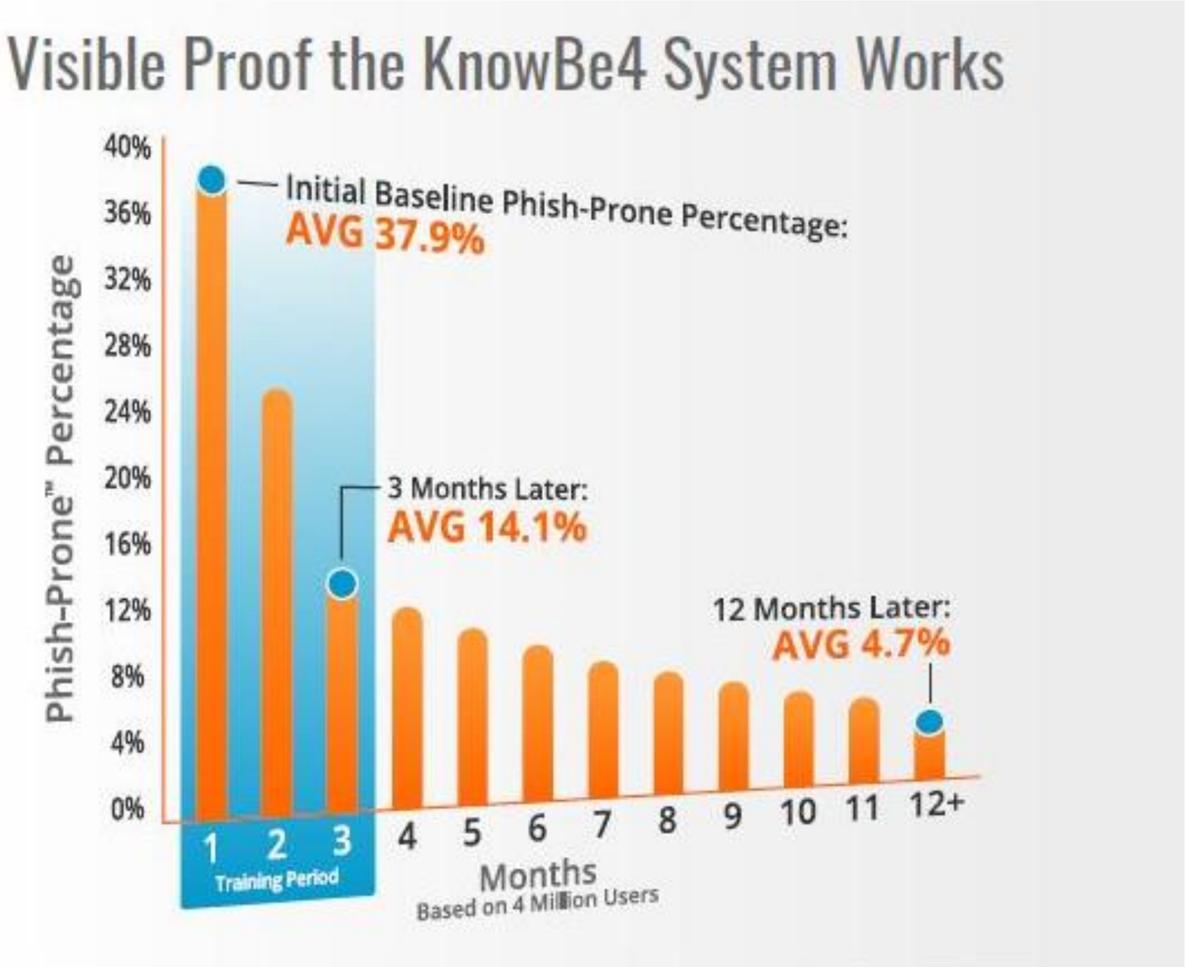
Enterprise-strength reporting, showing stats and graphs for both training and phishing, ready for management. Show the great ROI!



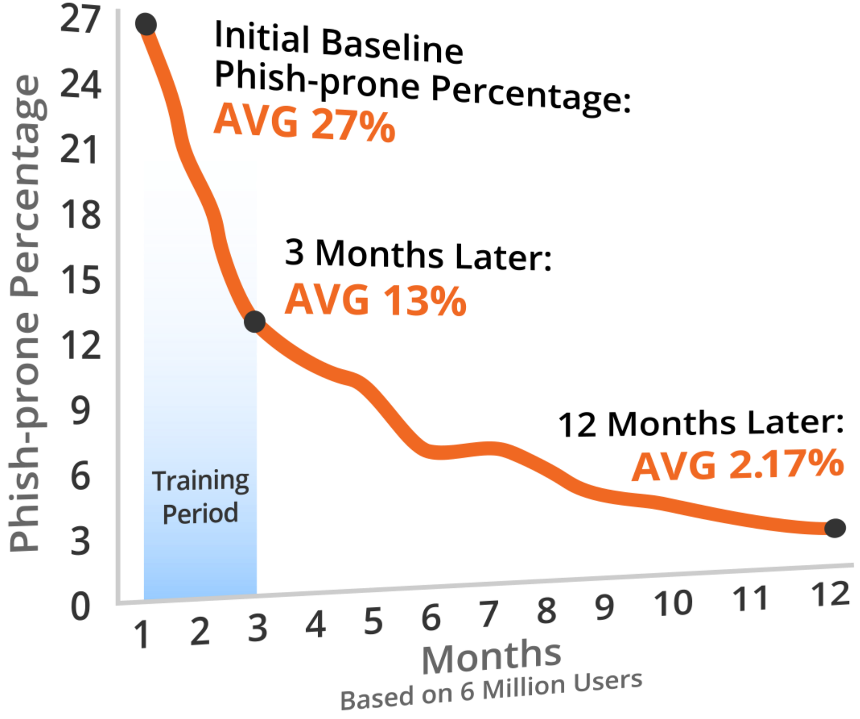
Security Awareness Training Program That Works

- Drawn from a data set of **over four million users**
- Over **17K organizations**
- **Over 9.1M** Simulated Phishing Campaigns
- Segmented **by industry type** and **organization size**

https://info.knowbe4.com/phishing-by-industry-benchmarking-report



Metrics, Videos, Posters, Gamification, and more



Consider using gamification and incentives to encourage friendly competition across departments.

Your metrics and reporting help tell your story.

Make everything reinforce your <u>point</u> and <u>purpose</u>

Security Awareness Training Cycle

Train Like You’re Marketing

- Frequent
- Redundant
- Entertaining

Security Awareness Training Cycle

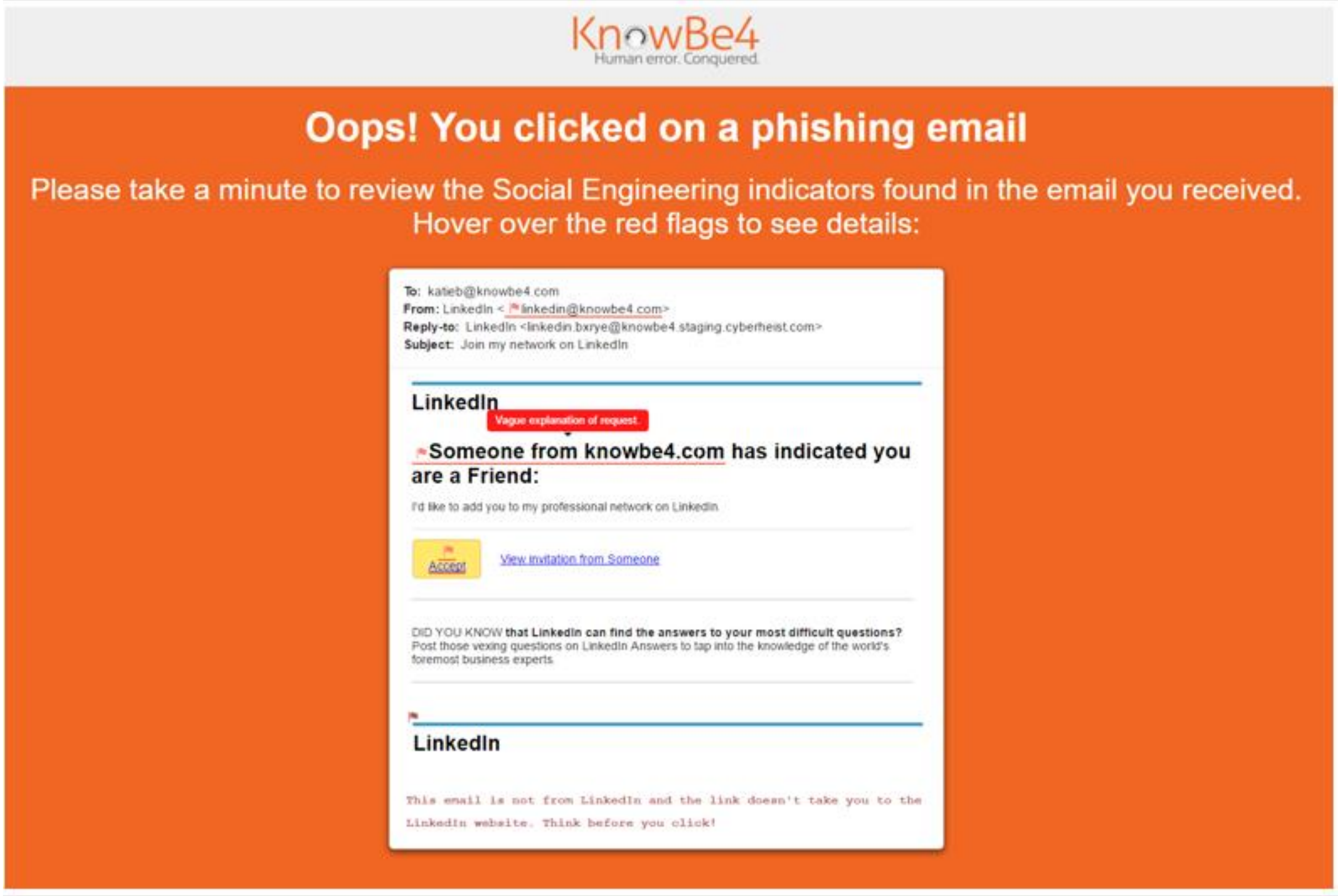
- When Hired
  - Acceptable Use Policy
  - Longer, Broader Training
- Ongoing
  - Monthly simulated phishing attacks
  - Immediate training when a test is failed
  - Ongoing shorter trainings
- Annual – longer training
- More Training As Needed

Make It Relevant

- Per Group, Per Role
  - You want different training for your executives versus your front-line employees
- Times, Seasons, Events of the Year
  - Different seasons and events generate different types of phishing
- Mix in general topics
- Not just email
- Not just to protect work scenarios only

Give Them Immediate Feedback Training

- Use Social Engineering Indicators Training



KnowBe4
Human error. Conquered.

Oops! You clicked on a phishing email

Please take a minute to review the Social Engineering indicators found in the email you received.
Hover over the red flags to see details:

To: katieb@knowbe4.com
From: LinkedIn < linkedin@knowbe4.com>
Reply-to: LinkedIn <linkedin.bxrye@knowbe4.staging.cyberheist.com>
Subject: Join my network on LinkedIn

LinkedIn

Vague explanation of request.

Someone from knowbe4.com has indicated you are a Friend:

I'd like to add you to my professional network on LinkedIn

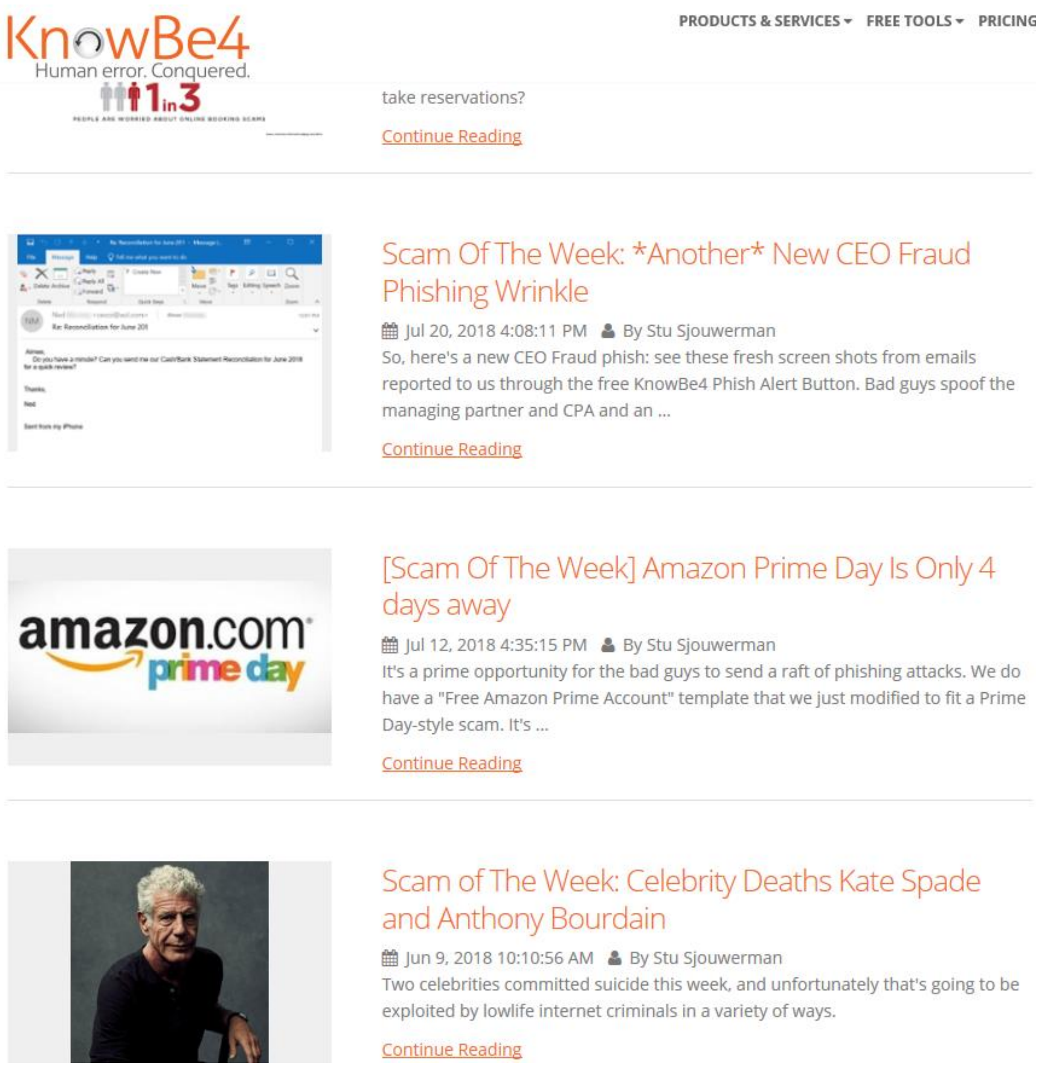
DID YOU KNOW **that LinkedIn can find the answers to your most difficult questions?** Post those vexing questions on LinkedIn Answers to tap into the knowledge of the world's foremost business experts

LinkedIn

This email is not from LinkedIn and the link doesn't take you to the LinkedIn website. Think before you click!

Keep Training Current

- Scams of the Week



take reservations?

Continue Reading

Scam Of The Week: *Another* New CEO Fraud Phishing Wrinkle

Jul 20, 2018 4:08:11 PM By Stu Sjouwerman

So, here's a new CEO Fraud phish: see these fresh screen shots from emails reported to us through the free KnowBe4 Phish Alert Button. Bad guys spoof the managing partner and CPA and an ...

Continue Reading

[Scam Of The Week] Amazon Prime Day Is Only 4 days away

Jul 12, 2018 4:35:15 PM By Stu Sjouwerman

It's a prime opportunity for the bad guys to send a raft of phishing attacks. We do have a "Free Amazon Prime Account" template that we just modified to fit a Prime Day-style scam. It's ...

Continue Reading

Scam of The Week: Celebrity Deaths Kate Spade and Anthony Bourdain

Jun 9, 2018 10:10:56 AM By Stu Sjouwerman

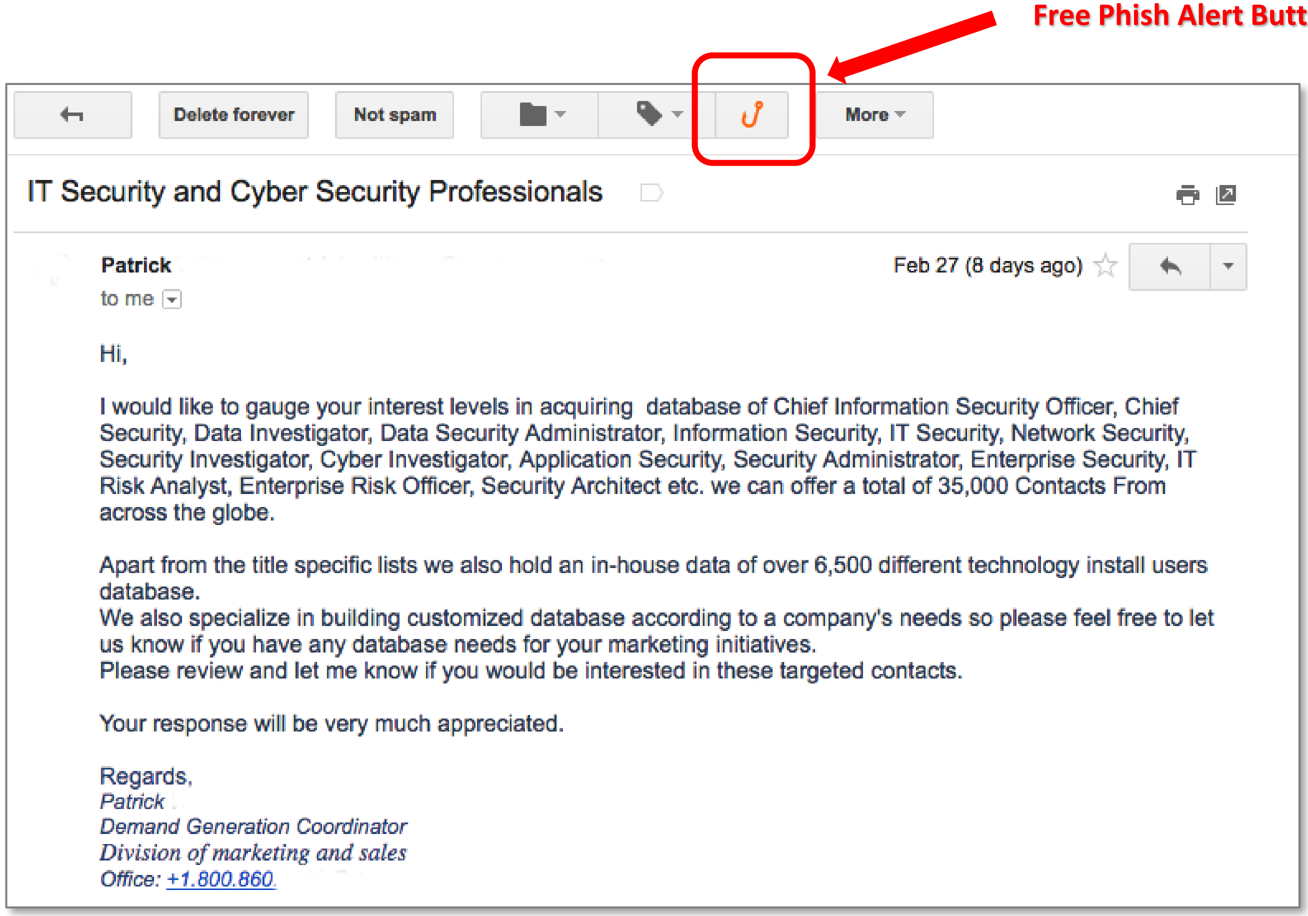
Two celebrities committed suicide this week, and unfortunately that's going to be exploited by lowlife internet criminals in a variety of ways.

Continue Reading

Give Users A Way To Report Attacks

- Give the users a way to provide the suspect email to someone that can review it

- “Train your employees with regard to phishing, and provide them with a quick and easy way to report suspicious emails.” 2017 DBIR



Free Phish Alert Button

IT Security and Cyber Security Professionals

Patrick
to me

Feb 27 (8 days ago)

Hi,

I would like to gauge your interest levels in acquiring database of Chief Information Security Officer, Chief Security, Data Investigator, Data Security Administrator, Information Security, IT Security, Network Security, Security Investigator, Cyber Investigator, Application Security, Security Administrator, Enterprise Security, IT Risk Analyst, Enterprise Risk Officer, Security Architect etc. we can offer a total of 35,000 Contacts From across the globe.

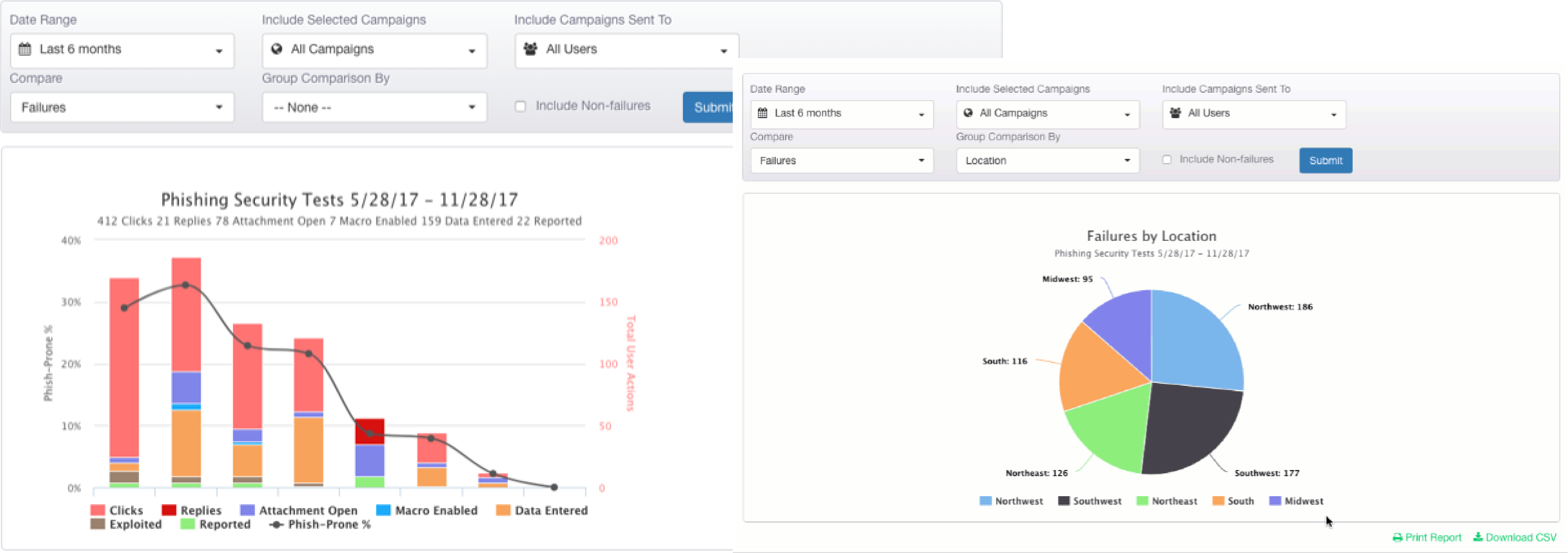
Apart from the title specific lists we also hold an in-house data of over 6,500 different technology install users database.
We also specialize in building customized database according to a company's needs so please feel free to let us know if you have any database needs for your marketing initiatives.
Please review and let me know if you would be interested in these targeted contacts.

Your response will be very much appreciated.

Regards,
Patrick
Demand Generation Coordinator
Division of marketing and sales
Office: +1.800.860.

Find Out Where the Weaknesses Are

- Get and Use Good Data



Date Range: Last 6 months
Include Selected Campaigns: All Campaigns
Include Campaigns Sent To: All Users
Compare: Failures
Group Comparison By: -- None --
☐ Include Non-failures

Date Range: Last 6 months
Include Selected Campaigns: All Campaigns
Include Campaigns Sent To: All Users
Compare: Failures
Group Comparison By: Location
☐ Include Non-failures

Best Practices

- Get senior management approval before conducting any simulated phishing tests
  - Surprises are not good
- Get beginning baseline and ongoing “phish-prone” statistics
- After initial baseline, communicate testing and training strategy to all users
  - It’s a part of the training and changing the culture
- Randomize the phishing times and subjects
  - Avoid sending out every phish test in one big blast
- Do group-, topic-, news-, and season-specific testing mixed in with broad, general categories (e.g. free donuts, etc.)

Resources

Free IT Security Tools

Domain Doppelgänger

Awareness Program Builder

Domain Spoof Tool

Mailserver Security Assessment

Phish Alert

Ransomware Simulator

Weak Password Test

Phishing Security Test

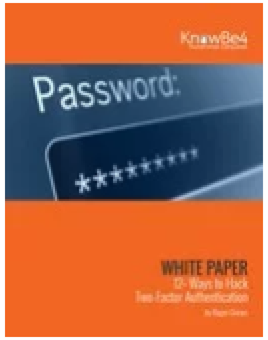
Second Chance

Email Exposure Check Pro

Training Preview

Breached Password Test

Whitepapers



12+ Ways to Hack Two-Factor

All multi-factor authentication (MFA) mechanisms can know how to defend against MFA hacks? This whitepa those attacks.

Ransomware Hostage Rescue Manual

Get the most complete Ransomware Manual packed with actionable info that you need to have to prevent infections, and what to do when you are hit with ransomware.

CEO Fraud Prevention Manual

CEO fraud is responsible for over $3 billion in losses. Don't be next. The CEO Fraud Prevention Manual provides a thorough overview of how executives are compromised, how to prevent such an attack and what to do if you become a victim.

» Learn More at www.KnowBe4.com/Resources «

Thank You!

Questions?

Roger A. Grimes– Data-Driven Defense Evangelist, KnowBe4
rogerg@knowbe4.com
Twitter: @rogeragrimes
LinkedIn: www.linkedin.com/in/rogeragrimes