Phishing, Vishing, & Smishing: How can I protect my business from these threats?

Tonia Dudley
Director, Security Solution Advisor

Mitchel Chang
Vice President, Corporate Social Responsibility & Education

@staysafeonline
✓ Convening partners who recognize strength in the security collective

✓ Educating individuals & organizations on cybersecurity best practices

✓ Amplifying collective efforts to increase cybersecurity awareness

www.staysafeonline.org

@staysafeonline
Thanks to our National Sponsors

Signature Sponsor
TREND MICRO

Affiliate Sponsor
education

Strategic Partner
IDENTITY PROTECTION SERVICES

Over 6,000 webinar attendees
Over 5,000 workshop attendees
Over 15,000 subscribers

"This was an excellent webinar with good information for small businesses and tech support companies like us who provide advice on support and security to our customers. The information covered can be passed along to our customers so they are CyberAware!"
Today’s Guest Speakers

Tonia Dudley
Director, Security Solution Advisor

Mitchel Chang
Vice President, Corporate Social Responsibility & Education

(MODERATOR)
Daniel Eliot
Director of Education & Strategic Initiatives
National Cyber Security Alliance

*This webinar will be recorded and will be distributed to registrants after the webinar concludes*
Poll

1) How confident do you feel in identifying a malicious email or text yourself?

2) Do you think your employees/colleagues are knowledgeable enough to identify a malicious email or text message?
Tonia Dudley

Director,
Security Solution Advisor

THIS IS COFENSE
AT-A-GLANCE...

END-TO-END PHISHING DEFENSE POWERED BY OVER 22M HUMANS

22M+ Active Reporters
150M Simulations Delivered
2000+ Enterprise Customers
150+ Countries Served

PHISHME
REPORTER
TRIAGE
VISION
INTELLIGENCE

Copyright © 2020, Cofense. All rights reserved.
TYPES OF PHISHING.

- URL Link
- Credential
- Attachment
WARNING SIGNS OF A PHISH.

1. Unknown Sender.
2. Emotional Appeal.
4. URL Link.
5. Solicits Sensitive Info.

From: christopher.mccoy@intlpackagedelivery.com
Subject: ATTENTION REQUIRED: TROUBLE WITH YOUR ORDER

This is an automatic notification: you must go through this letter to claim the item.

Follow the URL seen down below to use our recently implemented tracking system.

Order 3251351

Enter your username password tracking number to verify the account.

All the best,
Christopher McCoy - Chief Support Manager.
WARNING SIGNS OF A SMSISH.

1. Unknown Sender.
2. Emotional Appeal.
4. URL Link.
5. Solicits Sensitive Info.
Coronavirus Update

Hello redirected

Please let me know if I can be of further assistance to you.

Thanks

FOLLOW UP ON COVID-19

Encrypted file
View Online & Download

Adobe PDF Online

Sign in

Tactic Image w/ Link | Threat: Credential Phish | SEG: O365 | Proofpoint
You missed a call for COVID-19 Update

VM <person@example.com>
To: <you@example.com>

If there are problems with how this message is displayed, click here to view it in a web browser.

You have a new Voicemail:

From: (866) 618-8586
Received: Monday, March 30, 2020
Length: 00:27 Seconds
To: (redacted@professionalervices.com)

To listen to this message, Listen/Download VM here: http://info.sansung.usa.com/?id=3308f47f0b1-proj0938070.disk.com

Thank you for using Cisco Messaging System.
Click or tap to follow link.
COVID-19 Update

Hello Everyone!

Please see the information attach on the latest information/hotline number for the COVID-19 pandemic we are experiencing. Please become familiar with this information and any other resources available. Please be safe

Vincent
Safety Manager
THREAT TYPE: CREDENTIAL THEFT

- Word > OneNote
- Preview Document
- Login

THREAT TYPE: BEC/CEO FRAUD

- Typical BEC tactic
- No URL
- No Attachment

INFO CENTER: https://cofense.com/remote-work
THREAT TYPE: BEC/CEO FRAUD

INFO CENTER: https://cofense.com/remote-work
THREAT TYPE: MALICIOUS

• Keyloggers:
  ▪ HawkEye (RAR, Zip)
  ▪ Agent Tesla (PDF)

• RAT:
  ▪ Sonbokli (Zip)
  ▪ GuLoader (Zip)

• Ransomware:
  ▪ Nemty (bit.ly link)

WHAT TO DO.

• Keep Work & Personal separate – where possible

• Keep Devices Updated!

• Protect you CREDS

• Use caution
TRENDS.

- Finance Related
- Credential Phish
- Multiple Layers

3) What is the frequency of employee security training at your job?
Mitchel Chang
Vice President, Corporate
Social Responsibility & Education

https://resources.trendmicro.com/Coronavirusresources.html#News
Trend Micro
A world safe for exchanging digital information

- Cybersecurity focused for 30+ years
- Profitable since going public in 1998, with over $1.5B in sales (FY2019)
- 500,000+ commercial customers
- 6700+ people passionate about security across 65+ countries

Eva Chen, CEO & Co-founder Trend Micro
Cybercrime Increased by 300%!

According to FBI on April 20, 2020, instances of cybercrime appear to have jumped by as much as 300 percent since the beginning of the coronavirus pandemic. The bureau’s Internet Crime Complain Center (IC3) is now receiving between 3K to 4K cybersecurity complaints per day, up from the average 1K per day before.

**Opportunities for cyber criminals**

- America’s daily activities increasingly moving online
- Newly remote workers unaware of basic security measures
- Companies struggling to keep externally-accessed systems secured
- Lack of social and work place interactions
- Ongoing uncertainties:
  - Supply chains (PPE and essential goods)
  - Online orders and payments
  - Medical help and COVID-19 testing
  - Fears and other factors….
Monthly spam email detections
(containing covid, covid-19, coronavirus, or ncov)

*Note that the detection numbers represent the coverage of our Smart Protection Network sensors, which have limited global distribution.

This data reflects findings from January 1 to March 31, 2020.
Instances that malicious COVID-19 related URLs were accessed

*Note that the detection numbers represent the coverage of our Smart Protection Network sensors, which have limited global distribution. This data reflects findings from January 1 to March 31, 2020.
COVID-19-Related Threats in Q1 2020

- **907K**
  - Total spam messages related to COVID-19

- **737**
  - Detected malware related to COVID-19

- **48K**
  - Hits on malicious URLs related to COVID-19

- **220x**
  - Increase in spam from Feb to Mar 2020

- **260%**
  - Increase in malicious URL hits from Feb to Mar 2020

**United States**

Top location for spam and malware detections, and users accessing malicious URLs

*Detection numbers are based on the coverage of our Smart Protection Network, which has a limited global distribution (collection period January 1 to March 31, 2020).*
Threat Defense for SPAM and Phishing

- SPAM
- Phishing
- SMS/text/SM (Smishing)
- Voice (Vishing)
- Email
- Mobile & infra security

Cloud, Hybrid, or Data Centers
Office
Home/Individual

Social media block
misinformation

SPAM
Threat Defense for SPAM and Phishing

SPAM

Cloud, Hybrid, or Data Centers

Office

Home/Individual

SPAM

Mobile Carrier Security

SMS/text/SM (Smishing)

Voice (Vishing)

Email

Phishing

$$$
Mobile Web, App, and SMS Blocking Example
Important:
User Awareness, Education, and Behavior
Business Email Compromise (BEC)

On April 6, 2020, Federal Bureau of Investigation (FBI) issued a warning anticipating a rise in BEC schemes related to the COVID-19 Pandemic.

“Fraudsters will take advantage of any opportunity to steal your money, personal information, or both. Right now, they are using the uncertainty surrounding the COVID-19 pandemic to further their efforts.”

According to FBI, there has been an increase in BEC frauds targeting municipalities purchasing personal protective equipment in the fight against COVID-19. Also, most of the recent BEC attacks were targeted at the financial institutions or banks.
Organized BEC Attackers

- A typical BEC attack would be launched by email. The emails are either spoofed or compromised by the attackers. For example, an attacker may pretend to be a vendor by requesting invoice or transaction payments.

- BEC attacker’s typical steps
  - Assessing to identify potential targets by using various searches in social media and on Internet sites
  - Creating a target list and send out phishing or spear phishing emails
  - Responding if the victim responds, engaging directly with some small exchanges to secure the fraud
  - Requesting financial transition by sending the money to a third party
  - Closing and repeating the same scam if possible
BEC Preventive Measures (recommendation)

- Avoid posting any personal identifiable information (PII) on Internet. For example, your birthday, Social Security or driver’s license number.
- Lessen the posting of any internal company or communities’ social activities to the public
- If you are not technically savvy, always leverage your IT person to check email headers if in doubt.
- Have a strong company policy and process
- Use cybersecurity tools
Protecting your business cybersecurity hygiene fundamentals review
Best Practices – Device Security

- Computers/Servers
- **Mobile Devices**
- Wi-Fi Routers
- Other Devices

- Update operating system and apps regularly
- Use built-in security features
- Turn off any app permissions you do not use
- Minimize location access
- Disable Bluetooth when not required
- Do not connect to unsecured Wi-Fi networks
- Only download apps from trusted sources
- Ignore and block unsolicited calls and messages. Do not return calls from unknown numbers
- Use long, strong passwords
- Minimize personal data in apps and websites
- Consider using a vendor security product
Best Practices – User Security

- Passwords
- Email Safety
- Online Safety
- Remote and office

- Cyber defense is no longer just behind your home or business network firewall
  ✓ Protecting your data is a must (versus just perimeter)
- Be cautious with public Wi-Fi
  ✓ Disable auto-join or auto-connect to popular public WiFi AP (i.e., airports, coffee shops, malls, restaurants)
  ✓ Understand how to use VPN and https
- Cloud service security and backup setup
  ✓ (One-Drive, Google Drive, Dropbox..etc.)
- Back-up strategy and process <= **Important**
  - On-premise and/or cloud
Trend Micro endpoint solutions such as the Smart Protection Suites and Worry-Free™ Business Security detect and block the malware and the malicious domains it connects to.

Trend Micro™ Email Security thwarts spam and other email attacks. The protection it provides is constantly updated, ensuring that the system is safeguarded from both old and new attacks involving spam, BEC, and ransomware.

Trend Micro Deep Discovery™ Email Inspector detects and blocks ransomware spear phishing emails through advanced analysis techniques for known and unknown attacks.


A multilayered protection is also recommended for protecting all fronts and preventing users from accessing malicious domains that could deliver malware.
Additional Resources

SCORE
http://score.org

National Cyber Security Alliance (NCSA)
https://staysafeonline.org/
https://staysafeonline.org/cybersecure-business/

Cybercrime Support Network (CSN)
https://cybercrimesupport.org/

COVID-19 information from various Trend Micro Research and Education
www.trendmicro.com (coronavirus banner) or
https://resources.trendmicro.com/Coronavirusresources.html
Thank You
Daniel Eliot
Director of Education & Strategic Initiatives

Vishing (Voice Phishing)

When someone tries to trick you into giving them your private information via a phone call.
Common Vishing Examples

- **Debt relief and credit repair scams**
  Scammers will offer to lower your credit card interest rates, fix your credit, or get your student loans forgiven if you pay their company a fee first.

- **Business and investment scams**
  Callers might promise to help you start your own business and give you business coaching, or guarantee big profits from an investment. Don’t take their word for it.

- **Charity scams**
  Scammers like to pose as charities. Scams requesting donations for disaster relief efforts are especially common on the phone. Always check out a charity before you give, and don’t feel pressured to give immediately over the phone before you do.

- **“Free” trials**
  A caller might promise a free trial but then sign you up for products — sometimes lots of products — that you’re billed for every month until you cancel.

- **Tech Support**
  Caller claims to be your tech support and wants to remote into your computer to fix it.
Steer Clear of the Vish

✓ Never give personal information over the phone
✓ Verify to clarify
✓ Know your contacts
✓ Establish policies and procedures
✓ A pre-recorded message doesn’t make the call more legitimate.
✓ Train employees

Be suspicious.
Politely hang up, then look up the organization’s customer service number on their official website and call that number rather than the number provided in the solicitation email or phone call.
Reporting Scams and Phishing Attempts

DHS Cybersecurity & Infrastructure Security Agency: https://www.us-cert.gov/report-phishing


Learn More: https://www.consumer.ftc.gov/articles/0208-phone-scams
Upcoming Webinars

- **May 26**: COVID-19 Scams
- **June 9**: Telework Security
- **July 14**: Business Identity Theft

Register here: [https://staysafeonline.org/event_category/cybersecure-my-business/](https://staysafeonline.org/event_category/cybersecure-my-business/)
Q&A

*This webinar will be recorded and will be distributed to registrants after the webinar concludes*