Social Engineering

14 November 2023

Coryn Mann BIO

Coryn D. Mann is the owner of Corvus Technologies, LLC. She has extensive experience in Subcontract Management, Supply Chain Management and Procurement. In her career Coryn has focused on serving the Federal Government for the past 25 years, leveraging her skills from 11 years of active-duty U.S. Air Force and 14 years of Defense Subcontracting services. She is dedicated to lowering cost and fostering competition using Subcontract Management best practices thru the Subcontract Lifecycle.

Coryn established Corvus Technologies, LLC with her husband Eric to combine their talents and provide subject matter expertise in the fields of Compliance, Cybersecurity, NIST SP 800-53, NIST SP 800-171 services & Subcontract Management services.

Eric Mann BIO

Eric A. Mann is the co-owner of Corvus Technologies, LLC. He has honed his Cybersecurity career and is a Subject Matter Expert (SME) with over 20 years combined experience in systems administration, enterprise computing optimization, systems certification and accreditation, systems hardening, vulnerability assessment, penetration testing, and information assurance. His diverse background helps to uniquely position Corvus Technologies, LLC for projects that bridge the gap between Compliance and Cybersecurity. Eric leverages experience and best practices from multiple industries while adhering to customer specific rules and regulations.

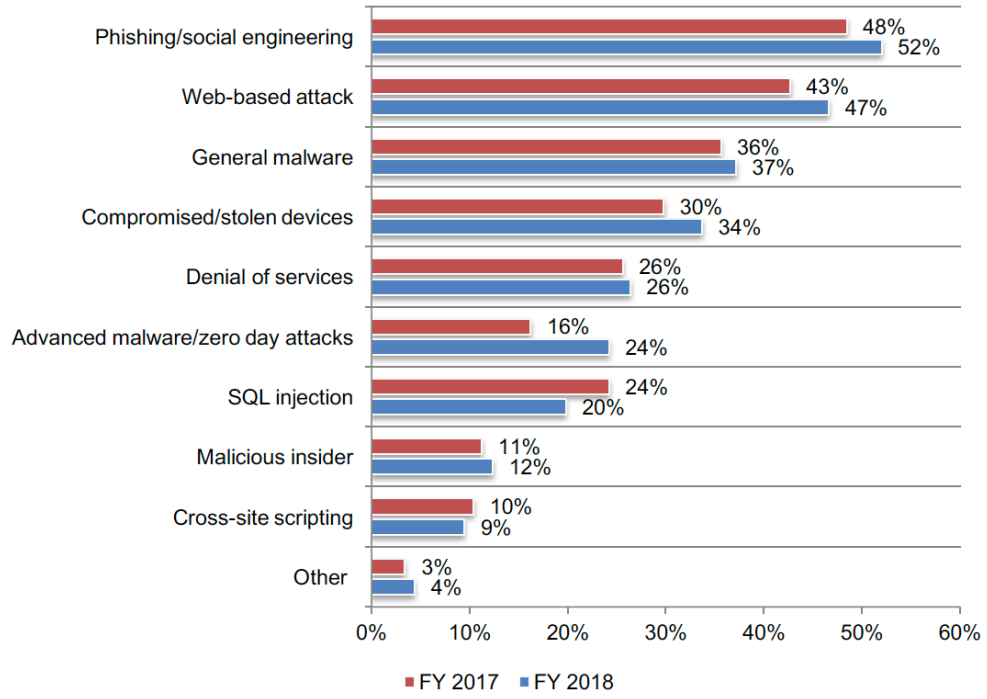
Eric established Corvus Technologies, LLC with his wife Coryn to combine their talents and provide subject matter expertise in the fields of Compliance, Cybersecurity, NIST SP 800-53, NIST SP 800-171 & Subcontract Management services.

Agenda

- Why Focus on Social Engineering?
- What is Social Engineering?
- Social Engineering Psychological Principles
- Social Engineering Information Gathering
- Social Engineering Attack Vectors
- Defense Against the Dark Arts
- How to Harden Your Organization
- Q&A (free-for-all)

Why Focus on Social Engineering?

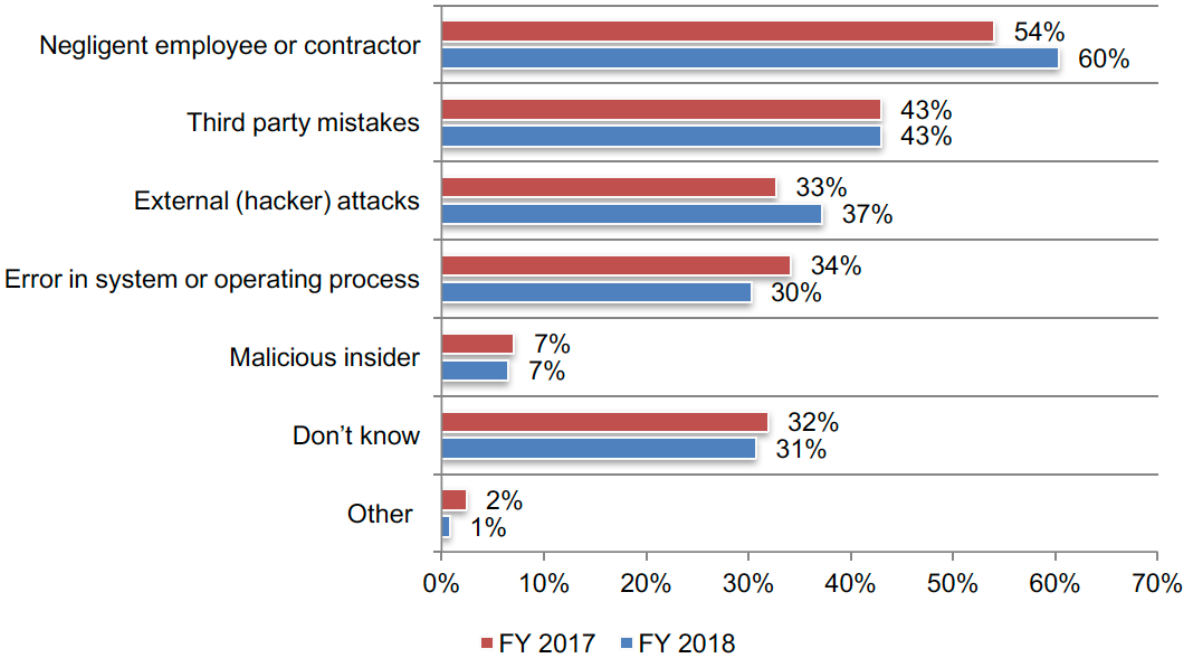
Figure 2. What types of attacks did your business experience?
More than one choice allowed



1-Source: Ponemon Institute, 2018 State of Cybersecurity in Small & Medium-Sized Businesses (SMB), November 2018

Why Focus on Social Engineering Continued

Figure 3. What was the root cause of the data breaches your business experienced?
More than one choice allowed



2-Source: Ponemon Institute, 2018 State of Cybersecurity in Small & Medium-Sized Businesses (SMB), November 2018

What is Social Engineering?

- **"You Can't Patch Stupid" – DEFCON**

- **General Definition** (https://www.social-engineer.org/about/):
  - "*Any act that influences a person to take an action that may or may not be in their best interest.*"

- **InfoSec Definition** (https://usa.kaspersky.com/resource-center/definitions/social-engineering):
  - *"…form of techniques employed by cybercriminals designed to lure unsuspecting users into sending them their confidential data, infecting their computers with malware or opening links to infected sites."*

What is Social Engineering Continued

- **Treated as a Scientific Discipline!**
  - https://www.social-engineer.org/
- **Topic is Neutral**
  - Morality/Legality based on implementation
- **Attacks human vs. machines:**
  - *Targets willingness to help/provide value*
  - *Shortcut to compromise!*

Social Engineering Psychological Principles

- **(Quickly) Establish Rapport:**
  - Choose Authority or Dependence/Sympathy
  - Establish Artificial Time Constraints
  - Modulate Voice Rhythm/Speed/Volume/Pitch (RSVP)
  - Stroke the Target's Ego
  - Complement/Validate the Target's responses
  - Ask How/Why/When

- **Create Human Buffer Overflow Condition**
  - Presupposition
  - Embedded Commands

Social Engineering Psychological Principles Continued

- **Frame the Conversation:**
  - Base on Target's Values/Expectations
- **Exert Influence:**
  - Utilize Authority
  - Establish Commitment and Consistency
  - Provide Concession/Demand Reciprocity (Quid Pro Quo)
  - Create Feeling of Scarcity
- **Elicit Information from Target**
- **Develop/Deliver Pretexted Persona**
  - Tailored to Target

Social Engineering Information Gathering

- **Utilizes Publicly available information:**
  - Business Cards
  - “Contact Us”
  - Business Records
  - Domain Registration
  - SOCIAL MEDIA
- **Demo Time!**
  - Whois:
    - https://www.whois.com/
  - Email Search
    - https://www.dossierc.com/

Social Engineering Attack Vectors

- **Phishing**
  - Email
- **Vishing**
  - Telephone
- **SMiShing**
  - Mobile Text Message Variant of Phishing
- **Impersonation**
  - Utilizes Established Pretext

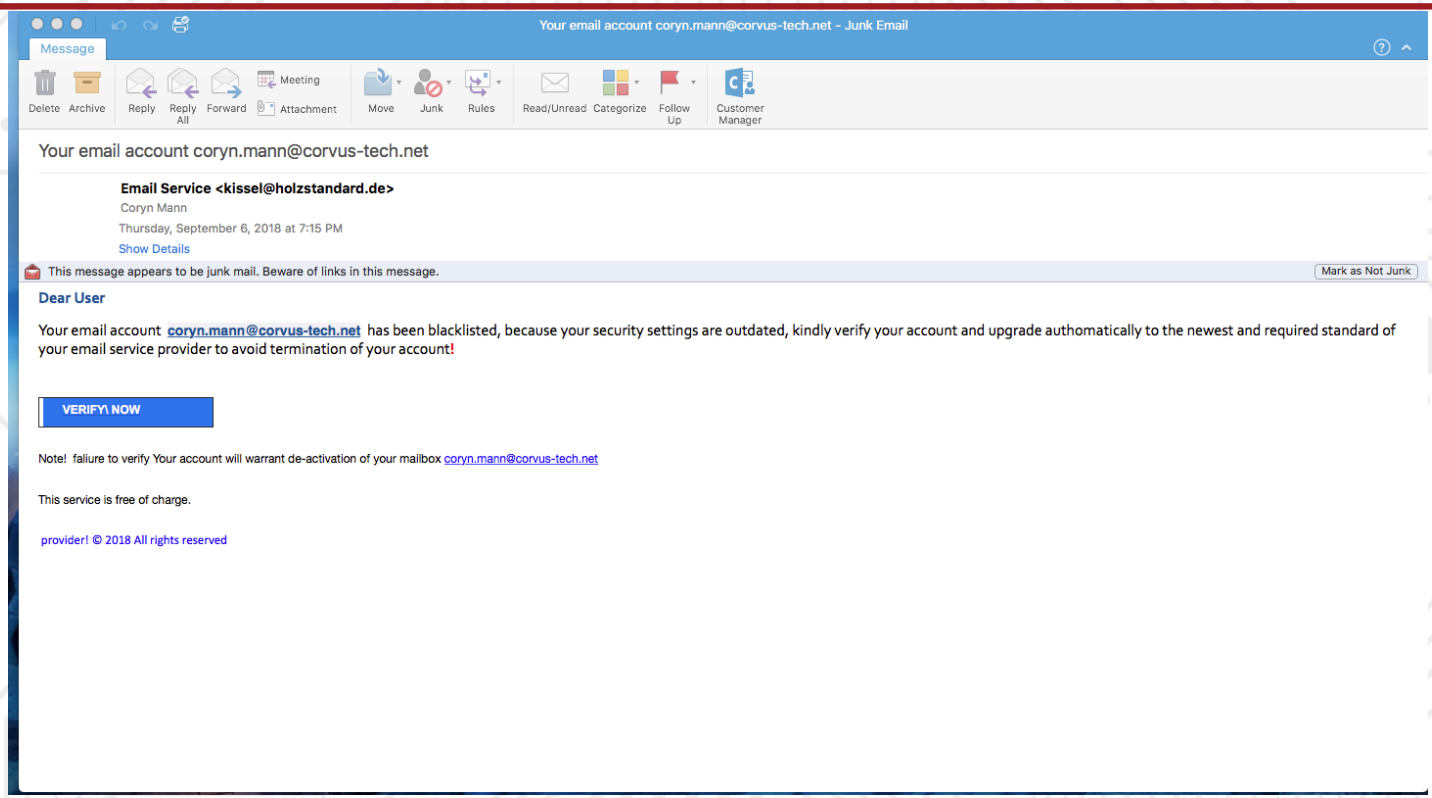
Phishing

- **Definition** (https://searchsecurity.techtarget.com/definition/phishing):
  - "Form of fraud in which an attacker masquerades as a reputable entity or person in email or other communication channels. The attacker uses phishing emails to distribute malicious links or attachments that can perform a variety of functions, including the extraction of login credentials or account information from victims."

Phishing Continued

- **Examples** (https://www.consumer.ftc.gov/features/feature-0038-onguardonline):
  - "We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity."
  - "During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."
  - "Our records indicate that your account was overcharged. You must call us withing 7 days to receive your refund."

Real-World Phishing Example 1



Your email account coryn.mann@corvus-tech.net - Junk Email

Message

Delete Archive Reply Reply All Forward Meeting Attachment Move Junk Rules Read/Unread Categorize Follow Up Customer Manager

Your email account coryn.mann@corvus-tech.net

Email Service <kissel@holzstandard.de>
Coryn Mann
Thursday, September 6, 2018 at 7:15 PM
Show Details

This message appears to be junk mail. Beware of links in this message. Mark as Not Junk

Dear User

Your email account coryn.mann@corvus-tech.net has been blacklisted, because your security settings are outdated, kindly verify your account and upgrade authomatically to the newest and required standard of your email service provider to avoid termination of your account!

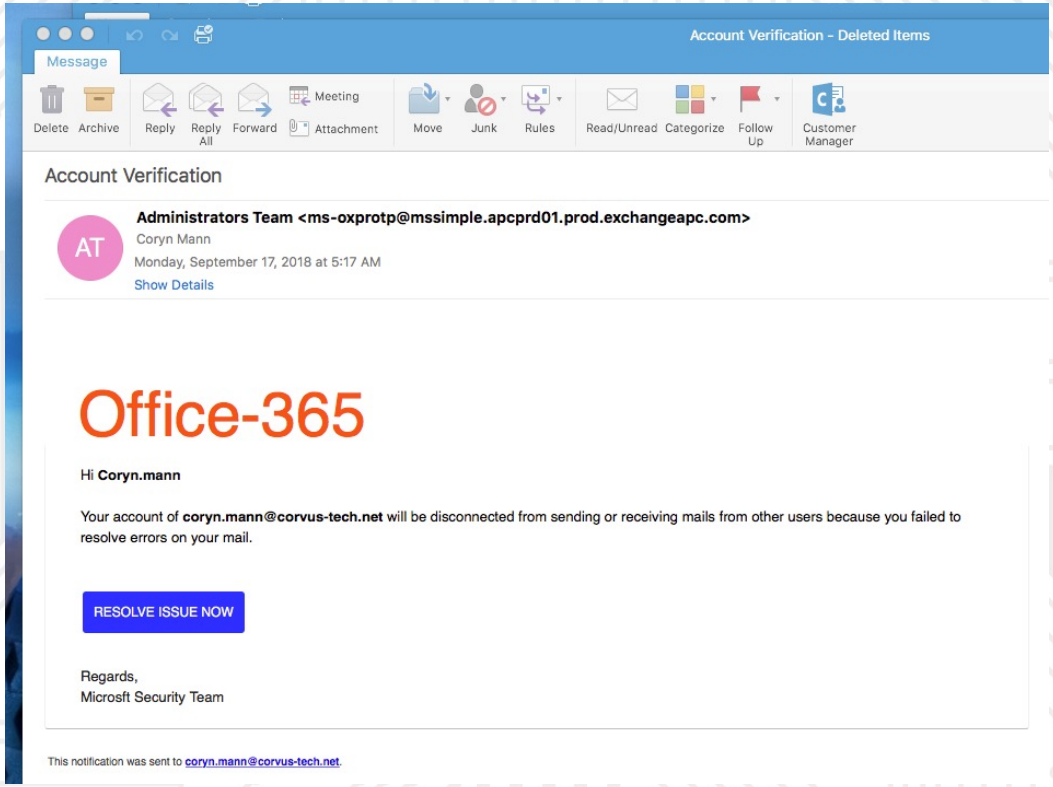
VERIFY\ NOW

Note! faliure to verify Your account will warrant de-activation of your mailbox coryn.mann@corvus-tech.net

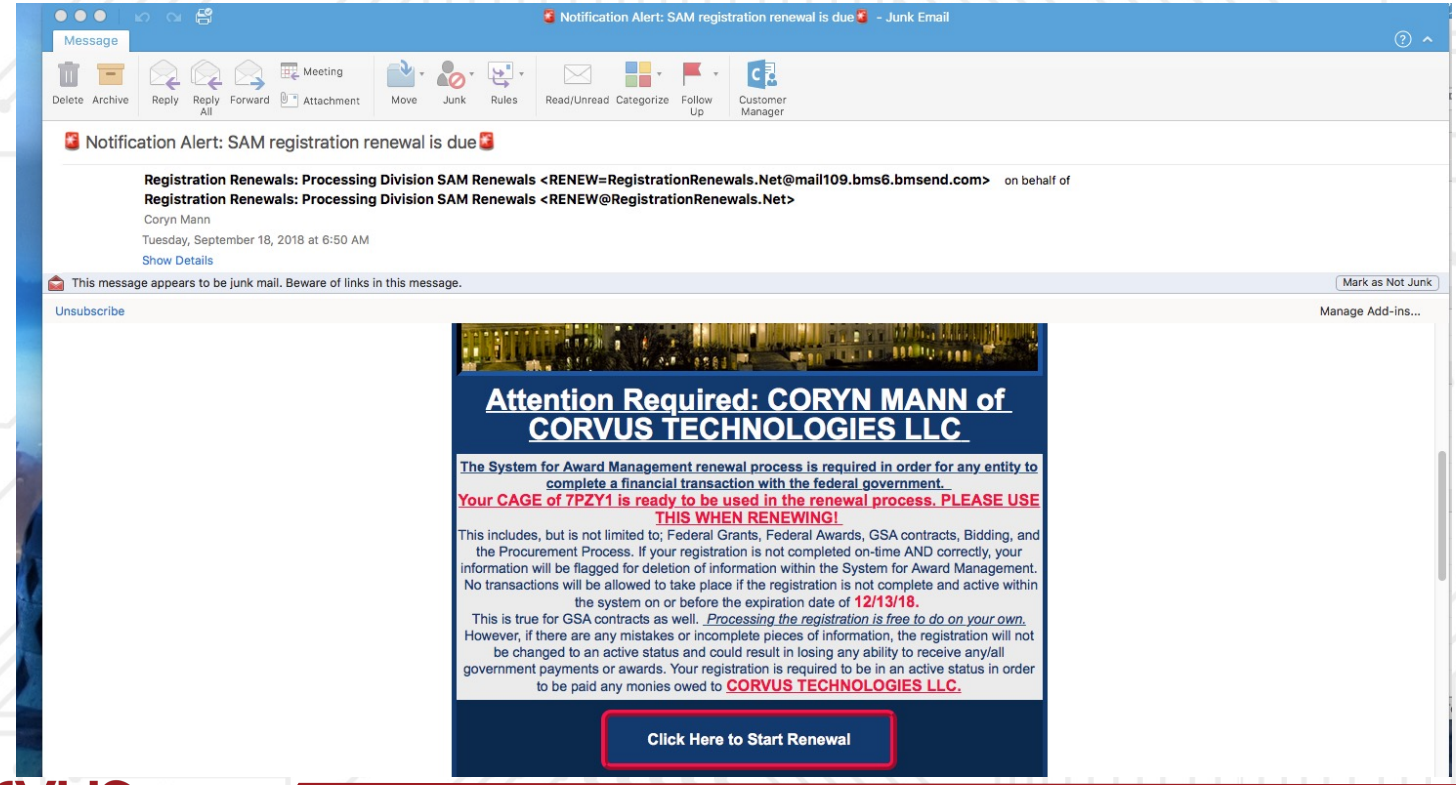
This service is free of charge.

provider! © 2018 All rights reserved

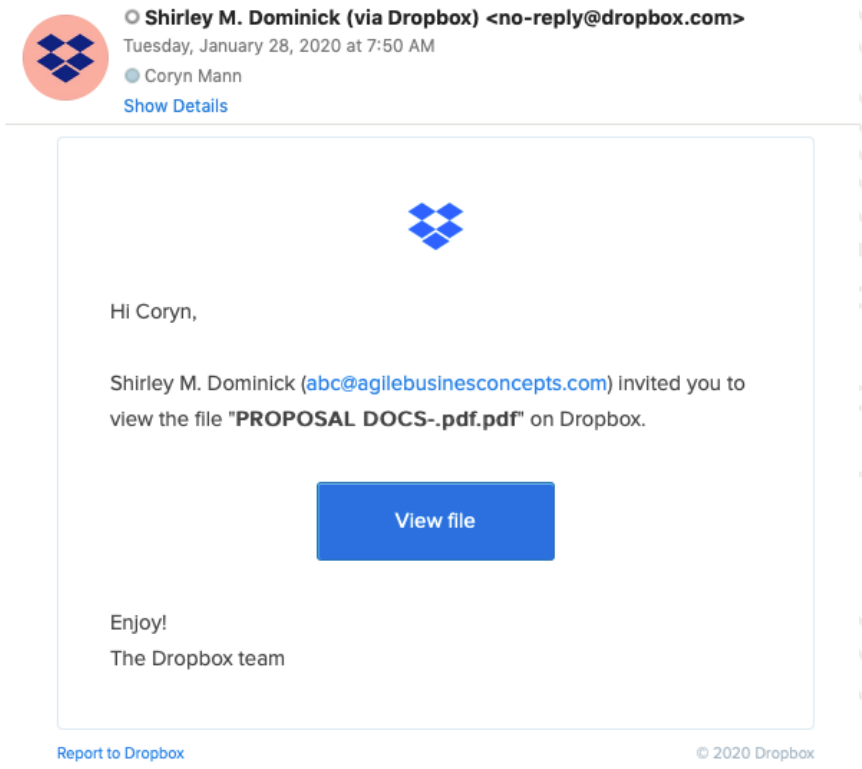
Real-World Phishing Example 2



Real-World Phishing Example 3



Real-World Phishing Example 4



Shirley M. Dominick (via Dropbox) <no-reply@dropbox.com>
Tuesday, January 28, 2020 at 7:50 AM
Coryn Mann
Show Details

Hi Coryn,

Shirley M. Dominick (abc@agilebusinesconcepts.com) invited you to view the file "**PROPOSAL DOCS-.pdf.pdf**" on Dropbox.

View file

Enjoy!
The Dropbox team

Report to Dropbox

© 2020 Dropbox

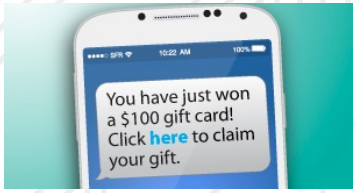
Phishing Variants

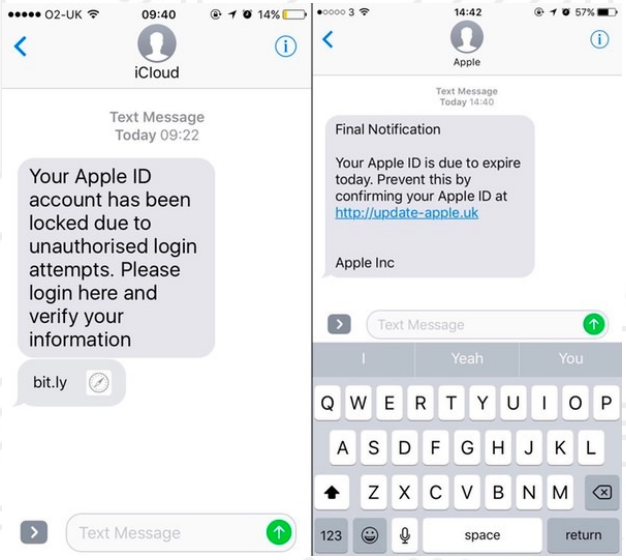
- Spear Phishing
- Whaling
- Pharming
- Vishing

Vishing in Action

- https://www.youtube.com/watch?v=lc7scxvKQOo

SMiShing Examples





Popular Impersonation Targets

- Tech Support
- Commercial Delivery Agent
- Postal Service*
- Law Enforcement*

Defense Against the Dark Arts

- **Phishing Defenses:**
  - Use Malware Protection/Prevention best practices
  - Never launch attachments!
  - THOROUGHLY examine Uniform Resource Locators (URLs) a.k.a Web Addresses:
    - Do not click on provided link
    - Examine link to test editor
    - Cut and paste in web browser (last resort!)

- **Vishing Defenses**
  - Verify identity of caller
  - Confirm allowable information disclosures with HR
    - Periodically train staff with updated information

Defense Against the Dark Arts Continued

- **SMiShing Defenses:**
  - DELETE
  - Utilize out-of-band contact methods:
    - Contact number located on back of card
    - Contact information listed on legitimate website

- **Impersonation Defenses:**
  - Establish / Enforce tech support contact procedures
  - Limit deliveries to secure reception area
  - Challenge / Deny access by default

Defense Against the Dark Arts Concluded

- **General Defensive Measures:**
  - Delay immediate response / action
  - Always vet information and sources
  - Route all requests to trained InfoSec staff
  - Immediately report all “suspicious” contacts to trained InfoSec staff
  - Maintain physical escort at all times
  - Provide compulsory awareness and education

How to Harden Your Organization

- **Test Your Organization:**
  - External vs. Internal test
  - Social Engineering Toolkit (SET)
- **Train Frequently (vs. Annually)**
  - Reinforces importance
  - Communicates commitment
- **Share Real-World "Inert" Samples With Organization:**
  - Provides situational awareness / validates threat
- **Maintain/Communicate Vigilance:**
  - Evil never sleeps!

Any Questions?

You can also reach us by phone or email.

eric.mann@corvus-tech.net

(888)-678-5039

5225 N. Academy Blvd.
Ste. 301
Colorado Springs, CO 80918

Coryn Mann | Owner
coryn.mann@corvus-tech.net

Eric Mann | Co-Owner
eric.mann@corvus-tech.net

888-678-5039
www.corvus-tech.net