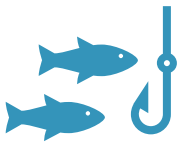
Phishing Workshop



Mini Lab1: GETTING STARTED

You've selected this workshop to learn more about phishing, perhaps you have the charter to develop a phishing program within your organization or looking to take your current program to the next level. We'll move through an understanding of your company and culture, teaming with stakeholders and supporting functional organizations and metrics to include reporting a phish.

1) **Which industry does your company work within? (Please circle)**

Accounting	Legal
Agriculture	Logistics & Supply Chain
Automotive	Manufacturing
Banking/Finance	Media & Entertainment
Business Services/Consulting	Metals & Mining
Chemicals	Nonprofit
Computer Services/Consulting	Pharmaceutical/Biotechnology
Consumer Electronics	Real Estate
Consumer Packaged Goods	Retail Trade
Education	Software
Energy	Technology
Engineering & Construction	Telecommunications
Food & Beverage	Transportation
Government / Public Sector	Travel & Tourism
Healthcare	Utilities
Hospitality	Other
Insurance	

2) **How many total employees does your company have (approx. 000's)?**

2a) Of these, how many are full-time employees?

2b) Of these, how many of these are contingent workers?

2c) Do you /will you, include contingent, seasonal, part time, contract employees in your training?

2d) Is your organization global, virtual and / or collocated? Consider any training, reporting and awareness requirements based on your demographic.

Lab2: SUPPORT TEAMS

As your building out the program, there will be many teams that will be impacted or need to be aware of the campaigns you are going to execute. This section will allow you to think about the various teams and the role they will play in your program. Your organization may have more functions that need to be consider, these are a place to start. Remember: everybody *thinks* they need to be included but keeping the "need to know" limited will help with making sure everyone benefits from the training.

1) How are your security, help desk and communications teams organized?

2) Do you have a SOC (Security Operations Center) or Incident Response team?

3) What is your Incident Reporting process? Do you instruct your users to report any type of security incident? Help Desk? Security?

4) How will you be obtaining email addresses? HR, Identity Access team, AD, LDAP

5) Are your Help Desk, email team and network teams staffed appropriately, and do they follow the sun (7/24-hour support)? This will address international and off hours support.

6) Technology:
   a) Spam Controls (Proofpoint / IronPort) _____
   b) URL Defense protection (no more hover) _____
   c) Attachment Defense (block certain types – macros, zip, .exe) _____
   d) Whitelisting vendor proxy filtering services (BlueCoat) _____

Lab 3: FRAMING YOUR PROGRAM

As your building out the program, it's important to set the framework for your program. This will help get the support you need to get approvals to begin the program and move forward. Developing your framework documentation will help realign your program if it gets of course.

1) Program Goal:
   a) What is your ultimate objective you're trying to achieve with your program (click vs report)

   b) Metrics (click / click & report / report)

   c) Will click information be shared with anyone in your organization?

2) Start with a Pilot – how many / business group (support) – creates a baseline to measure and gain support

3) Executive sponsor signoff?

4) Communications – do you introduce the program ahead of time – or follow up with results after (everyone, management, executive)

5) Planning your first campaign – start small and build.
   a) By business

   b) By location

   c) By function / role

6) Frequency:
    a) Monthly
    b) Quarterly
    c) How many scenarios / campaigns

7) Selecting your campaign scenarios: What type of emails get past your perimeter controls (i.e. what does your SOC or Threat Intelligence teams see).

    a) Start simple (may take some leadership convincing – technical leaders think it's TOO easy)

    b) URL vs Attachment

    c) Data Entry – this is for more mature programs – and maybe even targeted (privileged users)

    d) Languages – more advance

8) Selecting your Education
    a) Do you need to ensure you have language translations?

    b) Align to the scenario type
        i) URL – website content
        ii) Attachment
        iii) Data Entry

Lab 4: ADVANCING YOUR PROGRAM

Once you've established your program, there are steps you can take to advance and mature your program. The items below are various types of campaigns that you will want to set up to reduce the risk to the organization. There will be a point in your program when you have enough data to dig deeper and focus on high risk / high value targets.

1) New Hires – create a cadence to train (monthly / quarterly) – do you have access to hire dates (once matured the program, you have the data to support the need)

2) Repeats – setting a threshold – how many time
   a) Additional training
   b) Increase frequency

3) Board or Senior Leadership reporting: What are you reporting up to the board (metrics)?

4) Spearphish campaigns to targeted risk groups
   a) HR – W2 timing
   b) Finance – invoice
   c) Exec – BEC

RESOURCES

Below is a list of resource that provide some data points to support your program needs. These are just a few examples and some of the sources provide these updates to these reports quarterly or annually.

- Cofense (PhishMe): Enterprise Phishing Resiliency & Defense Report and Malware Review
  - https://cofense.com/whitepaper/enterprise-phishing-resiliency-and-defense-report/
  - https://cofense.com/whitepaper/malware-review-2018/
- KnowBe4: 2018 Phishing by Industry Benchmarking
  - https://info.knowbe4.com/2018-phishing-by-industry-benchmarking-report
- Proofpoint – The Human Factor Report and Quarterly Threat Report
  - https://www.proofpoint.com/us/human-factor-2018
  - https://www.proofpoint.com/us/resources/threat-reports/latest-quarterly-threat-research
- NIST Phishing Report (research report)
  - Public link
- STH Community – Phishing
  - https://sth-community.sans.org/category/phishing
- Verizon Data Breach Digest
  - http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest_xg_en.pdf
- Verizon Data Breach Investigations Report
  - https://www.verizonenterprise.com/verizon-insights-lab/dbir/
- Wombat: State of the Phish
  - https://www.wombatsecurity.com/state-of-the-phish