How To Improve Phishing Awareness by 300% in 18 Months

Emily Heath
Global CISO
AECOM
@CISOEmilyHeath
Setting the stage

AECOM Scope
Fortune 500 (#156)
$20 Billion Revenue
100,000 Employees
150 Countries Globally
Evidence shows that a staggering amount of incidents begin with phishing emails.

We decided to focus our education predominantly on phishing.

Using multiple channels and methods of awareness.

We reduced our “click rate” over 300% in 18 months.

Today I will share some of the ways we found that worked for us.
The Baseline

Simulated Phish sent to all employees globally

30% Click Rate!
After 18 Months…

Simulated Phish sent to all employees globally

6.7% Click Rate!
Who We Partnered With

- Executives
- Corporate Communications
- Marketing
- Graphics and Design
- Human Resources
- Your IT Colleagues
- Facilities / Office Management
- Other People of Influence
• Important to note that our phishing awareness campaign was augmented with other awareness activities
• Don’t just phish and expect changes
• Use the data to best of your ability
• Find ways to keep the conversation going regularly and engage with work force in multiple ways
• Look for positive reinforcement – i.e. when people report phishing emails, etc
Simulated phishing exercise to all employees
- Even though we send to 150 countries, we send in English, Russian and French
- Work with corporate communications on policies for your org
- When employees click the simulated phish – immediately takes them to educational site

CISO communication with “Clickers”
- Everyone who clicked goes into an email group
- Email explains why phishing awareness is important, and asks them to take phishing training
- BCC them.. No naming and shaming
- CISO mailbox account that can be managed by your team if needed

“Clickers” take phishing training

Chatter ‘theme’ each month with weekly CISO posts

Article in enterprise newsletter to augment the theme

Manager notes & security moments to augment the theme
Quarterly phishing results distributed to Executives in regions
  - Executives had been briefed by CISO before receiving these – important to set context and ask for help
  - Distribution includes “Top 10” office locations by region to make it more meaningful locally

Phishing results at region/country level shared on Chatter

Local campaigns based on phishing results – train the trainer
  - Local IT staff used to help with local campaigns – cyber briefings, postcards, local awareness etc

Security QBR with IT leaders
  - Not phishing related – but important to keep IT engaged
  - Include key partners like ERM, Internal Audit, etc

Security awareness poster to all offices placed in common areas
Annually

- Security awareness training annual program
  - All employees, try and make it mandatory
  - Work with HR, communications and training teams to help you with the delivery
- Training for all IT staff
  - Take responsibility to train the IT team. Not everyone is a security expert, help them understand why it matters, share real incidents, ask for their help
- Yearly lookback on phishing campaign
  - Annual results shared with regional executives and summaries posted on chatter as well as featured in corporate newsletters etc
Ad Hoc

• CISO in person Cyber Briefings
  • Try and meet face to face with employees wherever possible
• Executive briefings
  • You need executive support – help them understand why this is a business driver
• Tailored trainings / briefings
• Swag!
• Featured speaker in other peoples staff meetings
  • Offer yourself and your team to present at staff meetings, etc.
• Onboarding materials – set the tone for your organization
• Security moments – before every meeting
• Outlook Phishing Reporter Button – the best thing we ever did!!
Observations & Geographical Differences

- At first we received mixed responses from employees
  - Some Quotes....

- Soon became the normal, and became competitive
  - Some Examples....

- What we found in regions
  - Some Examples...

- Very important to consider cultural differences
  - Local materials in local languages really help
  - Make sure it’s not too US centric - Asia is different to Australia, different to UK, Middle East, India, etc..
  - Leverage local expertise to learn how people best respond
  - Examples

- Make it safe for people to run toward you, not away from you

- There is no shame in clicking a phish.. The shame is in not telling anyone about it!
Summary

- Talk about security to anyone who will listen – needed for cultural change
- Find your partners, you cannot do it alone
- Know your available channels
- Take ownership of training and educating everyone
- Not everyone is a cyber expert – make training relevant to them
- Use the click data to the best of your ability - people love statistics and competition!
- Have fun with it!
Things You Can Do to Apply It

Next Week
- Understand your statistics
- Talk Talk Talk about security
- Make it easy for people to contact your team with questions
- Make it easy for people to report phishing

3 Months
- Establish regular IT briefings
- Establish which channels are open to you to communicate with your employees
- Begin engaging with the employee population – chatter, articles, posters, etc.

6 Months
- Look at ways to do simulated phish
- Educate your company on their phishing statistics and turn it into education
- Look to implement the reporter button
Thank You!
Q&A