Best Practices and Future Direction of Security Awareness Training

Erich Kron
Security Awareness Advocate, KnowBe4, Inc.
About Erich Kron

- CISSP, CISSP-ISSAP, MCITP, ITIL v3, etc…

- Former Security Manager for the US Army 2nd Regional Cyber Center – Western Hemisphere

- Former Director of Member Relations and Services for (ISC)²

- A veteran of IT and Security since the mid 1990’s in manufacturing, healthcare and DoD environments
About Us

- 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
- Former Gartner Research Analyst, Perry Carpenter is our Chief Evangelist and Strategy Officer
- 300% growth year over year
- We help thousands of organizations manage the problem of social engineering

Over 24,000 Customers

Inc. 500

[Inc. 500 Logo]

[Pie Chart showing industry distribution: Banking 19%, Technology 15%, Consulting 8%, Education 4%, Energy 7%, Government 7%, Finance 16%, Insurance 6%, Healthcare 7%, Manufacturing 11%]
Phishing: By The Numbers
A staggering 91% of successful data breaches started with a spear phishing attack.

Employees Are the Last Line of Defense

- 91% of successful data breaches started with a spear phishing attack.
- Ransomware is predicted to exceed damages of $11.5 billion and continues to grow.
- Spear-phishing emails were used by 71% of attack groups in 2017.
- In March 2018, 1 in 484 emails to organizations with 251-500 employees had malware.
There was a huge

8,500%

Increase in file-based cryptocoin miners on endpoints in 2017

Cryptominers Use Your Resources For Their Profit

- In 2017 file-based detections of coin miners on endpoint machines grew 8,500% over 2016
- Xbash is ransomware and a botnet on Linux and a cryptominer and worm on Windows
In 2017 Ransomware grew 300% over 2016.

Ransomware is predicted to exceed damages of $11.5 billion by 2019, and continues to grow.

Mobile malware variants increased by 54% in 2017.
CEO Fraud and BEC Causes $12.5 Billion in Damages

There are various versions of the scams. Victims range from large corporations to tech companies to small businesses to non-profit organizations. Many times, the fraud targets businesses that work with foreign suppliers or regularly perform wire transfer payments.

- Law enforcement globally has received complaints from victims in every U.S. state and in at least 150 countries.
- FBI Alert Number I-071218-PSA puts the losses at over $12.5 billion between October 2013 and May 2018.
- Between December 2016 and May 2018, there was a 136% increase in identified losses.
Recent studies show that over 54.9% of users click on a phishing link in under 60 minutes.

When Do People Click On Phishing Links?

- <= 60 mins: 54.91%
- 60 to 120 mins: 12.38%
- 120 to 180 mins: 7.23%
- 180 to 240 mins: 5.18%
- Up to 17 hours: 20.29%
Users: Arm Them For Battle
Just because I’m aware doesn’t mean that I care.

Security Awareness and Secure Behavior are NOT the Same Thing
Traditional awareness efforts are based on the belief (or hope) that information leads to action.

In other words ... the problem with awareness is that "awareness" itself does not automatically result in secure behavior.
We need to **condition people** to have the **right reflexive behaviors**

“Everybody has a plan until they get punched in the mouth.”

- Mike Tyson
5 Best Practices to Embrace

1. Have explicit goals before starting
2. Decide what behaviors you want to shape – choose 2 or 3 and work on those for 12 – 18 months
3. Treat your program like a marketing campaign, with relevant information
4. Phish frequently, at least once a month
5. Don’t be a jerk (i.e. don’t alienate people)
5 Best Practices to Embrace

1. Have explicit goals before starting
2. Decide what behaviors you want to shape – choose 2 or 3 and work on those for 12 – 18 months
3. Treat your program like a marketing campaign, with relevant information
4. Phish frequently, at least once a month
5. Don’t be a jerk (i.e. don’t alienate people)
Before beginning:

Be **completely honest** with yourself about your **goals** and what your current **organizational culture** will tolerate.
5 Best Practices to Embrace

1. Have explicit goals before starting
2. Decide what behaviors you want to shape – choose 2 or 3 and work on those for 12 – 18 months
3. Treat your program like a marketing campaign, with relevant information
4. Phish frequently, at least once a month
5. Don’t be a jerk (i.e. don’t alienate people)
The “Magic Wand” Thought Experiment

If you could wave a magic wand and instantly change three security behaviors in your organization, what would they be?
Why Is Getting the Desired Behaviors So Difficult?

3 truths about human nature: We're lazy, social, and creatures of habit. Design products for this reality.
10:59 AM - 31 Mar 2011
5 Best Practices to Embrace

1. Have explicit goals before starting
2. Decide what behaviors you want to shape – choose 2 or 3 and work on those for 12 – 18 months
3. Treat your program like a marketing campaign, with relevant information
4. Phish frequently, at least once a month
5. Don’t be a jerk (i.e. don’t alienate people)
Make It Relevant

• Stuffing users in to a break room once a year, feeding them coffee, donuts and PowerPoint slides will not change their behavior in a noticeable way

• What is missing is the correct estimation of the adversary being faced and the degree of commitment an organization has to have to stave of attacks
A nudge, as we will use the term, is any aspect of the choice architecture that alters people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives. To count as a mere nudge, the intervention must be easy and cheap to avoid. Nudges are not mandates. Putting fruit at eye level counts as a nudge. Banning junk food does not.

_Nudge: Improving Decisions About Health, Wealth, and Happiness, 2008_
5 Best Practices to Embrace

1. Have explicit goals before starting
2. Decide what behaviors you want to shape – choose 2 or 3 and work on those for 12 – 18 months
3. Treat your program like a marketing campaign, with relevant information
4. Phish frequently, at least once a month
5. Don’t be a jerk (i.e. don’t alienate people)
Coordinate Training And Phishing Campaigns

• Training on its own, typically once a year, isn’t enough
• Simulated phishing of groups of employees on its own doesn’t work
• But together, they can be combined to greatly increase effectiveness
**Phish Like the Bad Guys**

**Conduct “Full Random” Phishing Attacks**

- Prairie dogging is when an employee notices a simulated phishing email and warns the others in the office about it. Or employees get used to the simulated campaigns, and learn to watch out for them.

- The way to guard against this is to use what are termed full random simulated phishing attacks.

- This entails the selection of random message delivery, and random phishing templates to gain a more accurate estimate of an organization’s likelihood to fall victim to phishing.
Personalize Emails

Just adding an employee’s first name isn’t enough. Personalization must be taken further.

- For example, add an attachment named, “Q4 Payroll” and make it look like it’s sent to them accidentally by referring to their supervisors name in the message.
- Another tactic is to split phishing email into groups such as by departments, or to tie phishing emails into topical or popular events.
- Test them with the latest social engineering tactics and current event templates.
5 Best Practices to Embrace

1. Have explicit goals before starting
2. Decide what behaviors you want to shape – choose 2 or 3 and work on those for 12 – 18 months
3. Treat your program like a marketing campaign, with relevant information
4. Phish frequently, at least once a month
5. Don’t be a jerk (i.e. don’t alienate people)
Your awareness program and content are the visible ‘face’ of your department to the rest of your company.
4 Steps To Success
Baseline Testing
We provide baseline testing to assess the Phish-prone™ percentage of your users through a free simulated phishing attack.

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!
New School Security Awareness Training Programs Work

- Drawn from a data set of **over six million users**
- Across **nearly 11K organizations**
- Segmented **by industry type** and **organization size**
- **241,762** Phishing Security Tests (PSTs)
Encouraging Data Demonstrates the Inherent Effectiveness of Consistency

KnowBe4 Study -- Jan, 2018

• Drawn from a data set of over six million users
• Across nearly 11K organizations
• Segmented by industry type and organization size
• 241,762 Phishing Security Tests (PSTs)
• Allowing for a ‘follow-the-user-result’ from initial PST baseline, to results after 90 days of combined CBT and phishing training, to the result after one year of combined phishing and CBT

<table>
<thead>
<tr>
<th>Industries</th>
<th>Size ranges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Energy &amp; Utilities</td>
<td>1 – 249</td>
</tr>
<tr>
<td>Financial Services</td>
<td>250 – 999</td>
</tr>
<tr>
<td>Business Services</td>
<td>1000+</td>
</tr>
<tr>
<td>Technology</td>
<td></td>
</tr>
<tr>
<td>Manufacturing</td>
<td></td>
</tr>
<tr>
<td>Government</td>
<td></td>
</tr>
<tr>
<td>Healthcare &amp; Pharmaceuticals</td>
<td></td>
</tr>
<tr>
<td>Insurance</td>
<td></td>
</tr>
<tr>
<td>Not For Profit</td>
<td></td>
</tr>
<tr>
<td>Education</td>
<td></td>
</tr>
<tr>
<td>Retail &amp; Wholesale</td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
</tr>
</tbody>
</table>

For this study, the approximate number of organizations in each size range were as follows:

1 – 249 employees (~8K organizations)
250 – 999 employees (~2K organizations)
1000+ (~1K organizations)
# Benchmark Phish Prone Percentage by Industry

<table>
<thead>
<tr>
<th>Industry</th>
<th>1 – 249 employees</th>
<th>250 – 999 employees</th>
<th>1000+ employees</th>
</tr>
</thead>
<tbody>
<tr>
<td>Energy &amp; Utilities</td>
<td>31.56</td>
<td>29.34</td>
<td>22.77</td>
</tr>
<tr>
<td>Financial Services</td>
<td>27.41</td>
<td>28.47</td>
<td>23.00</td>
</tr>
<tr>
<td>Business Services</td>
<td>29.80</td>
<td>31.01</td>
<td>19.40</td>
</tr>
<tr>
<td>Technology</td>
<td>30.68</td>
<td>30.67</td>
<td>28.92</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>33.21</td>
<td>31.06</td>
<td>28.71</td>
</tr>
<tr>
<td>Government</td>
<td>29.32</td>
<td>25.12</td>
<td>20.84</td>
</tr>
<tr>
<td>Healthcare &amp; Pharmaceuticals</td>
<td>29.80</td>
<td>27.85</td>
<td>25.60</td>
</tr>
<tr>
<td>Insurance</td>
<td>35.46</td>
<td>33.32</td>
<td>29.19</td>
</tr>
<tr>
<td>Not For Profit</td>
<td>32.63</td>
<td>25.94</td>
<td>30.97</td>
</tr>
<tr>
<td>Education</td>
<td>29.20</td>
<td>26.23</td>
<td>26.05</td>
</tr>
<tr>
<td>Retail &amp; Wholesale</td>
<td>31.58</td>
<td>30.91</td>
<td>21.93</td>
</tr>
<tr>
<td>Other</td>
<td>30.41</td>
<td>28.90</td>
<td>22.85</td>
</tr>
</tbody>
</table>

**27%**

Avg. Initial Baseline PPP across all industries and sizes

Average PPP by Size of Organization

<table>
<thead>
<tr>
<th>Org Size</th>
<th>Initial PPP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - 249</td>
<td>30.1 %</td>
</tr>
<tr>
<td>250 - 999</td>
<td>28.5 %</td>
</tr>
<tr>
<td>1000+</td>
<td>25.06 %</td>
</tr>
</tbody>
</table>
## Results after 1 Quarter of CBT and Phishing Testing

<table>
<thead>
<tr>
<th>Industry</th>
<th>1 – 249 employees</th>
<th>250 – 999 employees</th>
<th>1000+ employees</th>
</tr>
</thead>
<tbody>
<tr>
<td>Energy &amp; Utilities</td>
<td>12.53</td>
<td>13.31</td>
<td>13.40</td>
</tr>
<tr>
<td>Financial Services</td>
<td>10.01</td>
<td>9.09</td>
<td>14.53</td>
</tr>
<tr>
<td>Business Services</td>
<td>12.89</td>
<td>13.99</td>
<td>13.86</td>
</tr>
<tr>
<td>Technology</td>
<td>14.12</td>
<td>16.93</td>
<td>19.83</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>13.87</td>
<td>14.24</td>
<td>9.88</td>
</tr>
<tr>
<td>Government</td>
<td>13.13</td>
<td>12.76</td>
<td>7.90</td>
</tr>
<tr>
<td>Healthcare &amp; Pharmaceuticals</td>
<td>16.81</td>
<td>11.02</td>
<td>15.79</td>
</tr>
<tr>
<td>Insurance</td>
<td>13.39</td>
<td>16.49</td>
<td>13.23</td>
</tr>
<tr>
<td>Not For Profit</td>
<td>16.01</td>
<td>17.28</td>
<td>17.07</td>
</tr>
<tr>
<td>Education</td>
<td>16.95</td>
<td>17.16</td>
<td>22.56</td>
</tr>
<tr>
<td>Retail &amp; Wholesale</td>
<td>13.39</td>
<td>10.47</td>
<td>10.49</td>
</tr>
<tr>
<td>Other</td>
<td>14.86</td>
<td>16.37</td>
<td>19.97</td>
</tr>
</tbody>
</table>

**Baseline Phish Prone Percentage (B-PPP)**

**13.3%**

**Avg. 90 Day PPP**

across all industries and sizes

Average PPP by Size of Organization

<table>
<thead>
<tr>
<th>Org Size</th>
<th>Initial PPP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - 249</td>
<td>13.11 %</td>
</tr>
<tr>
<td>250 - 999</td>
<td>13.20 %</td>
</tr>
<tr>
<td>1000+</td>
<td>14.10 %</td>
</tr>
</tbody>
</table>
## Results after 12 Months of CBT and Phishing Testing

### Baseline Phish Prone Percentage (B-PPP)

<table>
<thead>
<tr>
<th>Industry</th>
<th>1 - 249 employees</th>
<th>250 – 999 employees</th>
<th>1000+ employees</th>
</tr>
</thead>
<tbody>
<tr>
<td>Energy &amp; Utilities</td>
<td>2.83</td>
<td>1.87</td>
<td>5.56</td>
</tr>
<tr>
<td>Financial Services</td>
<td>1.54</td>
<td>2.22</td>
<td>5.81</td>
</tr>
<tr>
<td>Business Services</td>
<td>1.89</td>
<td>3.09</td>
<td>1.27</td>
</tr>
<tr>
<td>Technology</td>
<td>2.02</td>
<td>2.42</td>
<td>2.69</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>2.16</td>
<td>3.13</td>
<td>2.47</td>
</tr>
<tr>
<td>Government</td>
<td>1.87</td>
<td>1.46</td>
<td>1.52</td>
</tr>
<tr>
<td>Healthcare &amp; Pharmaceuticals</td>
<td>2.00</td>
<td>1.65</td>
<td>2.17</td>
</tr>
<tr>
<td>Insurance</td>
<td>2.23</td>
<td>2.68</td>
<td>5.26</td>
</tr>
<tr>
<td>Not For Profit</td>
<td>2.47</td>
<td>2.24</td>
<td>3.01</td>
</tr>
<tr>
<td>Education</td>
<td>2.80</td>
<td>1.91</td>
<td>5.31</td>
</tr>
<tr>
<td>Retail &amp; Wholesale</td>
<td>2.14</td>
<td>1.87</td>
<td>2.68</td>
</tr>
<tr>
<td>Other</td>
<td>1.82</td>
<td>3.18</td>
<td>4.21</td>
</tr>
</tbody>
</table>

### Average PPP by Size of Organization

- **1 - 249 employees**: 1.94%
- **250 - 999 employees**: 2.21%
- **1000+ employees**: 3.04%

---

**Percentages are calculated for users who experienced a combination of CBT *and* at least 10 phishing tests.**
Resources

Free Domain Spoof Test
Find out now if hackers can spoof an email address of your own domain

Free CEO Fraud Prevention Manual
This 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

Free Phishing Security Test
Find out what percentage of your users are Phish-prone

Free Ransomware Simulator
RanSim will simulate 10 ransomware infection scenarios and show you if a workstation is vulnerable to infection

Free Phish Alert Button
Your employees now have a safe way to report phishing attacks with one click!

Free Weak Password Test
Weak Password Test gives you a quick look at the effectiveness of your password policies and any fails so that you can take action.

Learn More at www.KnowBe4.com/Resources
Thank You!

Erich Kron – Security Awareness Advocate
ErichK@KnowBe4.com
@KB4Erich