Countering the Attacks

Erich Kron
Security Awareness Advocate
KnowBe4
About Us

- The world’s largest library of security awareness training content with well over 8,500 customers
- Based in Tampa Bay, Florida, founded in 2010
- Chief Hacking Officer-Kevin Mitnick
- We help thousands of organizations manage the problem of social engineering

KnowBe4 Debuts at #139 on Inc 500 List of America’s Fastest Growing Private Companies
Who Am I?

• 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
Employees Are the Weakest Link in Network Security

• 91% of successful data breaches started with a spear phishing attack

• **CEO Fraud** (aka Business Email Compromise) causes $3.4 billion in damages

• **W-2 Scams** social engineer Accounting/HR to send tax forms to the bad guys

• **Ransomware** was a 1 billion dollar business in 2016
When Do End-Users Click on Phishing Links?

- 54.91% <= 60 mins
- 20.29% 60 to 120 mins
- 12.38% 120 to 180 mins
- 7.23% 180 to 240 mins
- 5.18% Up to 17 hours

KnowBe4
Increasing Confidence

• **Train Your Users** – This is our number one suggestion because it works. An untrained staff is an incident waiting to happen. Most technical solutions are reactive and respond after an attack. It is important to have them to minimize the damage, but we prefer to prevent the attack.

• **Have Weapons Grade Backups** – Backups do no good if they are encrypted by the ransomware, so they have to be isolated from the network.

• **Enclave the Network** – Marketing computers rarely need to have network access to the SQL servers or accounting systems.

• **Principle of Least Privilege** – Not everyone should be an administrator. The less access users have, the less malware can spread.

• **Monitor the Network** – Use a system like a SIEM or IDS to alert on malicious network behavior.

• **Keep Up With Patches** – OS and applications need to be kept patched.
How Can We Protect Our Current Businesses?

The answer is defense-in-depth.
Comprehensive Programs Work

- Most security awareness programs are still too superficial and done for compliance reasons.

- What is missing is the correct estimation of the adversary being faced and the degree of commitment an organization has to have to stave off attacks.
Develop a Coordinated Campaign

• 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
Make Your Users A Human Firewall

- Train your users to identify potential phishing emails
- Make them a Human Firewall
Give Your Users An Action

• Give the users a way to provide the suspect email to someone that can review it.
How Do You Manage Social Engineering Threats?

**Baseline Testing**
Perform baseline testing to assess the Phish-prone percentage of your users through a simulated phishing attack.

**Train The Users**
On-demand, interactive, engaging training with common traps.

**Phish The Users**
Perform simulated phishing attacks using templates representative of current events or threats.

**See The Results**
Create reports showing stats and graphs for both training and phishing. Focus on areas of improvement.
Baseline Phishing Test

• Security awareness training can be undermined due to difficulty in measuring its impact. “You can’t manage what you don’t measure”

• It is vital to establish a baseline on phishing click-through rates

• Send out a simulated phishing email to a random sample of personnel to find out the number that are tricked into clicking and this is your baseline Phish-prone percentage
Train Everyone

- In order to create a security culture and change the behavior of employees, they have to train everyone, from the board room to the lunch room, and include the training in the onboarding of every new employee.

- This should be interactive and create a thorough understanding of how cybercriminals operate.

- Employees need to understand the mechanisms of:
  - Spam
  - Phishing
  - Spear-phishing
  - Malware
  - Ransomware
  - Social engineering
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.

• Leverage information such as our “Scam of The Week” and “Reported Phishes of The Week” categories to continuously train users.
Phish Like the Bad Guys

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
Continue to Test Employees Regularly

• Even when testing confirms that phishing susceptibility has fallen to nominal levels, continue to test employees frequently to determine if anti-phishing training remains effective

• The bad guys are always changing the rules, adjusting their tactics and upgrading their technologies

• Analyze your phishing data. Continue to train and phish your users with more advance tactics such as attachments and data entering landing pages

• Over time, increase the difficulty of the attacks, we have hundreds of templates rates by difficulty from 1 to 5
New-School Security Awareness Training Works!

Initial Phish-prone Percentage: AVG 15.9%

Training Period

12 Months Later: AVG 1.2%
Resources

Free Ransomware Hostage Rescue Manual
Get the most complete Ransomware Manual packed with actionable info that you need to have to prevent infections, and what to do when you are hit with ransomware

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

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

Free USB Test
Find out now what your user’s reactions are to unknown USBs

» Learn More at www.KnowBe4.com/Resources «