Email Safety and Security: The Human Firewall

Erich Kron
Security Awareness Advocate, KnowBe4, Inc.

Christopher Ramos,
IT Network Security Officer, City of Ocala
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
A little bit about me...

• Christopher Ramos – IT Network Security Officer, City of Ocala

• Certified Ethical Hacker (CEH), Certified Advanced Security Practitioner (CompTIA CASP), Microsoft Certified Solutions Expert (MCSE)

• Working in various role in IT for over 10 years.

• Seeking Master of Science in Cyber Security and Information Assurance
About KnowBe4

- The world’s most popular integrated new-school Security Awareness Training and Simulated Phishing platform, over 9,000 customers
- Based in Tampa Bay, Florida, founded in 2010
- Chief Hacking Officer: Kevin Mitnick
- We help organizations manage the ongoing problem of social engineering
City of Ocala

- Employees over 900 workers
- Fiber optic network solutions to local businesses and residents.
- Provide electric, water, sewer, storm water, solid waste, fire services within city limits.
- Horse capital of the world.
Corporate vs Personal email

• RSA 2017: Google Research presented a study over 1 billion email messages that they reviewed and came to the following conclusion:
  • Corporate accounts on average receive 4.3 times more malware, are 6.2 times more likely to receive phishing lures, and are 0.4 less likely to receive spam.

A corporate inbox receives 4.3x more malware than an end-user inbox
91% of successful data breaches started with a spear phishing attack

Ransomware was a 1 Billion dollar criminal business in 2016, and continues to grow

CEO Fraud (aka Business Email Compromise) causes $5.3 billion in damages

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

As Employees, You Are The Last Line Of Defense
There was a **752% increase** in new ransomware families in 2016.

- Ransomware caused about **$1B in losses** in 2016.
- Over 153,000 users were hit by **mobile ransomware** in 2016.
Ransomware price tags shot up by a staggering 266 percent to $1,077 on average in 2016.

Less than half that paid (45%) got their information back.
Recent studies show that over 54.9% of users click on a phishing link in under 60 minutes.
Ransomware attacks cause downtime, data loss, possible intellectual property theft, and in certain industries a ransomware attack is now looked at as a possible data breach.
In the news

• May 12, 2017 new variant of "WannaCry" campaign hits the world
• Leverages a vulnerability developed by the NSA, and patched by Microsoft. (MS17-010)
• Affected 150 countries, tens of thousands of computers and networks in just a few hours.
  • Shutting down some hospitals in the UK, unable to access patient records
• Not a targeted campaign, all they wanted: $300
MalwareTech.com, WannaCry Tracker
Training

• Why is training important?
  • Don’t just use training videos

• Training Curriculum
  • Provide different types of training

• Remediation training

• Instant Training
  • On-click failure training

• Informational notices about current phishing campaigns.
How can we protect our current businesses?

Social Engineering Red Flags

**FROM**
- I don’t recognize the sender’s email address as someone I ordinarily communicate with.
- This email is from someone outside my organization and it’s not related to my job responsibilities.
- This email was sent from someone inside the organization or from a customer, vendor, or partner and is very unusual or out of character.
- Is the sender’s email address from a suspicious domain (like microsoft-support.com)?
- I don’t know the sender personally and they were not vouched for by someone I trust.
- I don’t have a business relationship with any past communications with the sender.
- This is an unexpected or unusual email with an embedded hyperlink or an attachment from someone I haven’t communicated with recently.

**DATE**
- Did I receive an email that I normally would get during regular business hours, but it was sent at an unusual time (e.g., 3 a.m.)?

**SUBJECT**
- Did I get an email with a subject line that is irrelevant or does not match the message content?
- Is the email message a reply to something I never sent or requested?

**TO**
- I was cold on an email sent to one or more people, but I don’t personally know the other people it was sent to.
- I received an email that was also sent to an unusual mix of people.
- For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

**HYPERSLINKS**
- I hover my mouse over a hyperlink that’s displayed in the email message, but the link to address is for a different website. (This is a big red flag.)
- I received an email that only has long hyperlinks with no further information, and the rest of the email is completely blank.
- I received an email with a hyperlink that is a misspelling of a known website. For instance, www.bankoffrance.com—the “r” is really two characters—and “f”.

**ATTACHMENTS**
- The sender included an email attachment that I was not expecting or that makes no sense in relation to the email message. (This sender doesn’t ordinarily send me this type of attachment.)
- I see an attachment with a possibly dangerous file type. The only file type that is always safe to click on is a .txt file.

**CONTENT**
- Is the sender asking me to click on a link or open an attachment to avoid a negative consequence or to gain something of value?
- Is the email out of the ordinary, or does it have bad grammar or spelling errors?
- Is the sender asking me to click a link or open an attachment that seems odd or illegal?
- Do I have an uncomfortable gut feeling about the sender’s request to open an attachment or click a link?
- Is the email asking me to look at a compromising or embarrassing picture of myself or someone I know?

© 2017 KnowBe4, LLC. All rights reserved. Other product and company names mentioned herein may be trademarks and/or registered trademarks of the respective companies.
Phish your employees

• Why should you phish your employees?
• How often should you phish your employees?
• Mix up your phishing test.
  • Include current events
  • Tailor to employee occupation
  • Include online service providers
  • Include known phishing campaigns

Warning ⚠ Don't Click!

Image source: thehackernews.com
Suspicious emails

• What do your employees do when they see a suspicious email in their inbox?

• Is there an easy way to report suspected phishing emails
  • Get everyone involved and promote culture of security
  • Make your employees sensors.

• If there is, is feedback given?
  • Positive reinforcement
Simulated vs Non-simulated

Total Emails Reported: 1376
Simulated Reported: 869
Non-simulated Reported: 507

Reporting of simulated vs non-simulated phishing emails
Last 30 days
Recent Sample Phishing Emails

• Presented as a secure .pdf document

• The document will have an embedded payload or a malicious link

• Usually designed to trigger concern or confusion
Recent Sample Phishing Emails

• Nobody like their bank account being messed with

• Most, if not all, of the links are to malicious websites

• Usually designed to trigger concern or confusion

• Spacing doesn’t quite line up and the cc: email is odd
Recent Sample Phishing Emails

- Who doesn’t want a free 50 bucks?
- Most, if not all, of the email links to a malicious website
- Usually designed to prey on the excitement of winning something of value
- In this case, the reply to address made no sense
[Phish Alert] Important Online Banking Alert

- Submitted by Mike Poucher on 2017-04-03 at 09:32 AM

Dear Valued Customer,

For your safety some information on your account appears to be missing or incorrect. Please click the link immediately and follow the step to re-confirm your information as we have on record.

Bank of America.
Spear phishing continued…

Email sent from Canadian Domain

Link redirects to malware site in Indonesia
Recent Attacks

Cockrell Hill Police Department, Texas

• “OSIRIS” variant of Locky ransomware infection causes the loss of 8 years of police department evidence

• The Chief said. “Our automatic backup started after the infection, so it just backed up infected files”

• The press release states that this is the result of a phishing email
Recent Ransomware Trends

Ransomware as a Service

• This is designed to let people that are not technical set up attacks

• Different ways of doing this, for example, Philadelphia is $400, Dot is free with a 50/50 split of profits.
Recent Ransomware Trends

Named Popcorn Time

• Offers free decryption if you infect 2 others and they pay

• Creators claim to be hackers from Syria trying to feed the hungry and clothe the poor
Recent Attacks

Licking County, OH

• Ransomware took online access and landline phones were down.

• More than 1,000 government computer systems shut down.

• 911 center computers were down and they had to log contacts manually.

• County auditor Mike Smith found a bright side and said, “Apparently, our clock still works.”
How it’s changed the City of Ocala

• Initial baseline test: 25% click rate
• Current average: ~4% click rate
• Security Awareness posters placed in communal areas.
• Friendly reminder emails.
• Over the last year, 4700 simulated emails have been sent.
• Introduction of a Phish button to report suspected malicious emails
Phishing Security Tests

Phishing Security Tests 4/18/16 – 5/18/17

337 Clicks 1 Replies 14 Attachment Open 0 Macro Enabled 29 Data Entered 988 Reported

Phish-Prone %

Total User Actions

Clicks  - Replies  - Attachment Open  - Macro Enabled  - Data Entered  - Exploited

Reported - Phish-Prone %
What if you’ve been compromised?

• Does your company have an incident response policy or team?
• Has there been any preparation?

• Security controls; Tools for detection and analysis
  • Containment, eradication, and recovery
• Post incident activity Lessons learned
Is it malicious?
Baseline Testing
We provide baseline testing to assess the Phish-prone™ percentage of your users through a free simulated phishing attack.

Train Your Users
On-demand, interactive, engaging training with common traps, live Kevin Mitnick demos and new scenario-based Danger Zone exercises and educate with ongoing security hints and tips emails.

Phish Your Users
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!
Thank You!

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

Christopher Ramos
IT Network Security Officer
http://www.ocalafl.org/
https://www.facebook.com/cityofocalafl/
(352) 629-CITY

Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Sales@KnowBe4.com