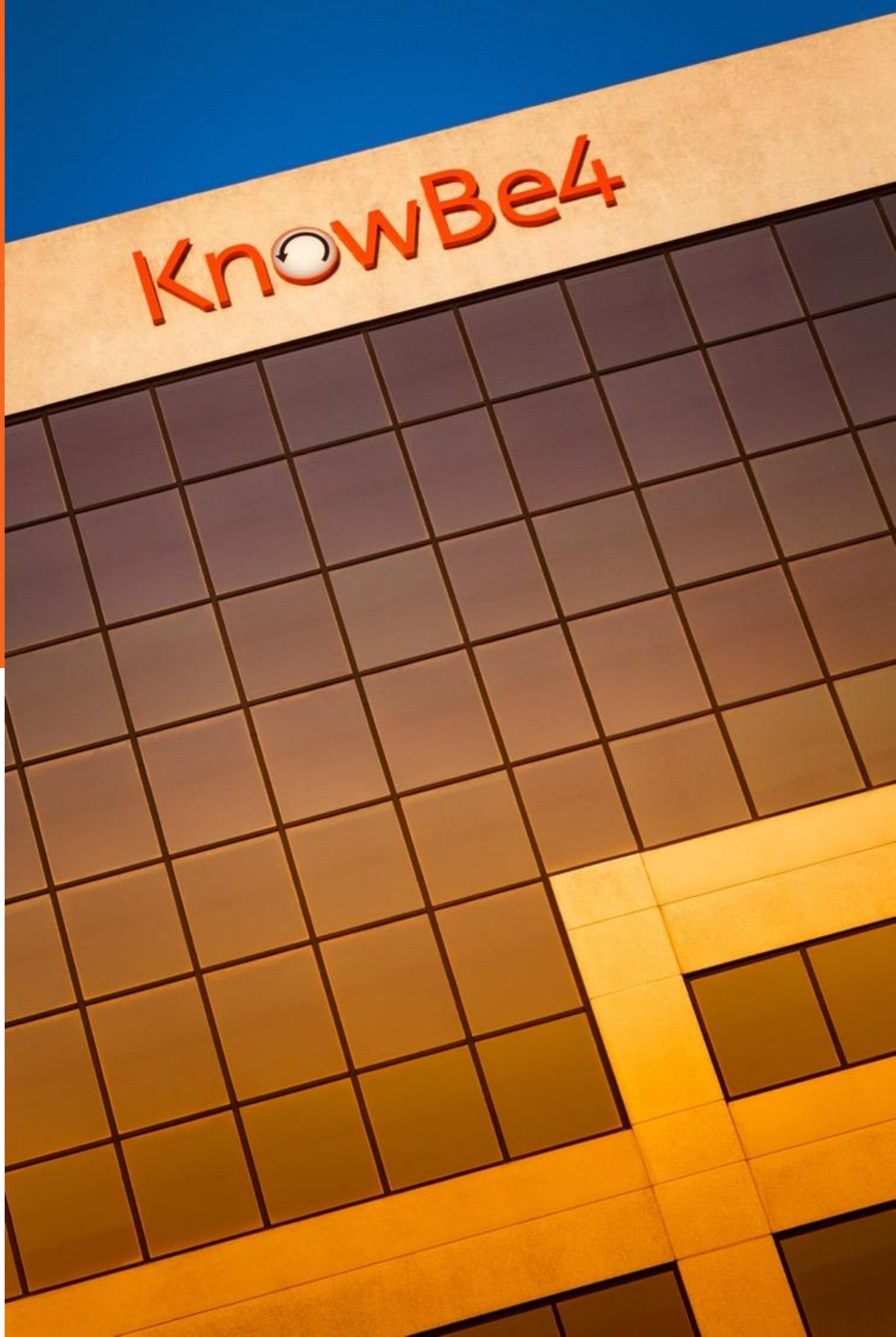
Countering the Attacks

Erich Kron

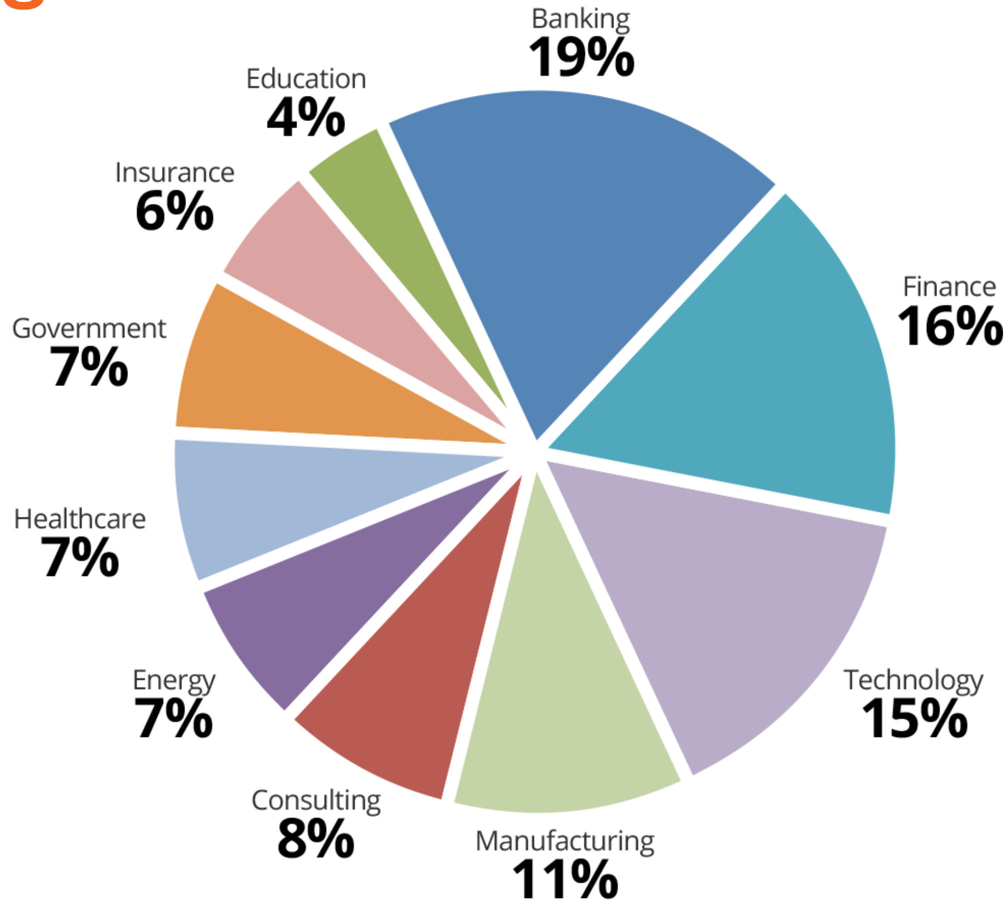
Security Awareness Advocate

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



Inc. 500

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

CISSP® Certified Information Systems Security Professional

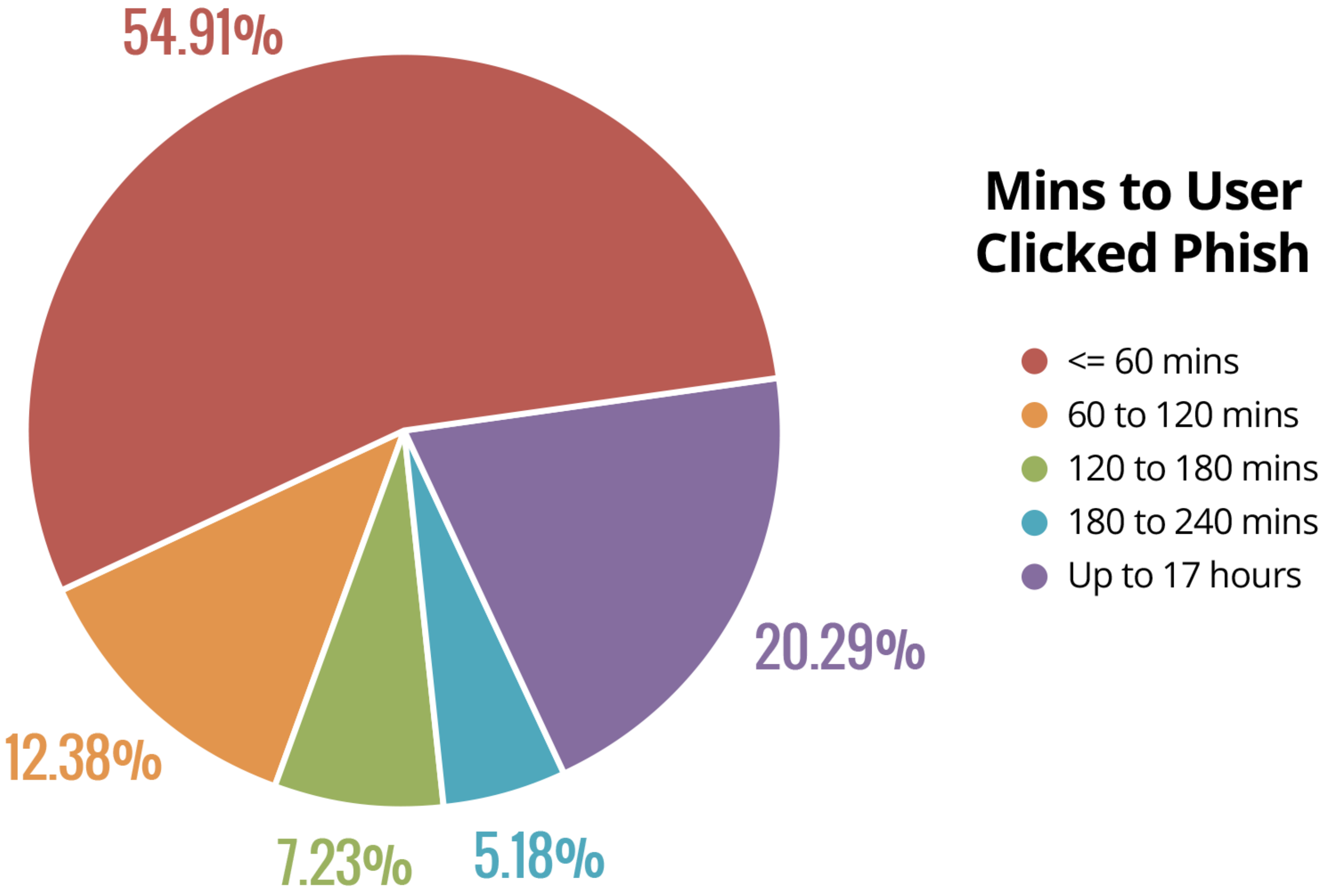
CISSP® Certified Information Systems Security Professional
ISSAP® Architecture

Microsoft® CERTIFIED IT Professional

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?

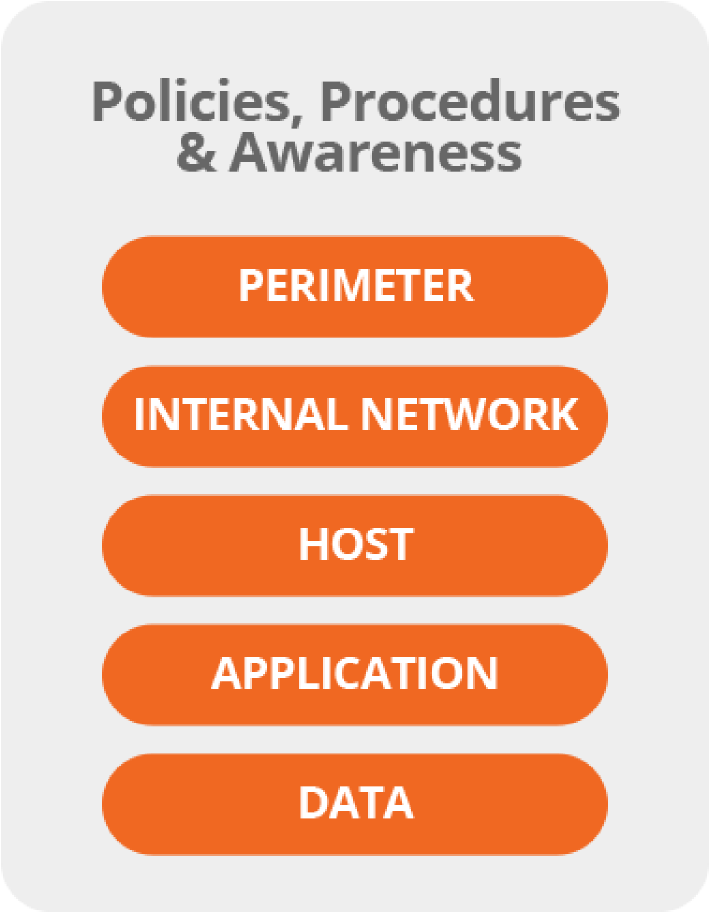


Increasing Confidence

- **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.



Policies, Procedures & Awareness

PERIMETER

INTERNAL NETWORK

HOST

APPLICATION

DATA

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 of attacks

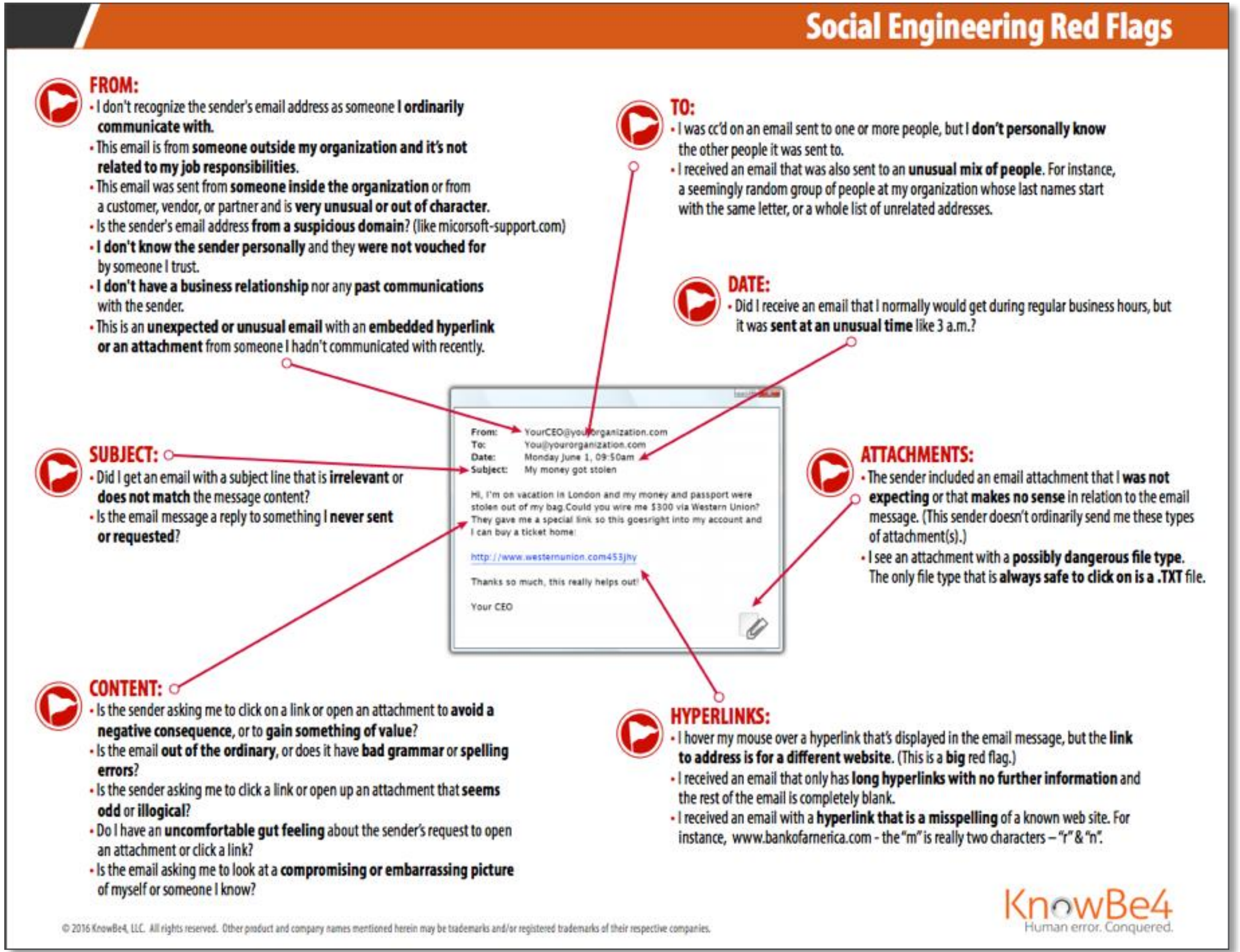
Develop a Coordinated Campaign

- 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



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 micorsoft-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** nor any **past communications** with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I hadn't communicated with recently.

TO:

- I was cc'd 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, a seemingly random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

DATE:

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 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?**

From: YourCEO@yourorganization.com
To: You@yourorganization.com
Date: Monday June 1, 09:50am
Subject: My money got stolen

Hi, I'm on vacation in London and my money and passport were stolen out of my bag.Could you wire me $300 via Western Union? They gave me a special link so this goesright into my account and I can buy a ticket home:

http://www.westernunion.com453jhy

Thanks so much, this really helps out!

Your CEO

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 these types of attachment(s).)
- 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 up an attachment that **seems odd** or **illogical?**
- 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?

HYPERLINKS:

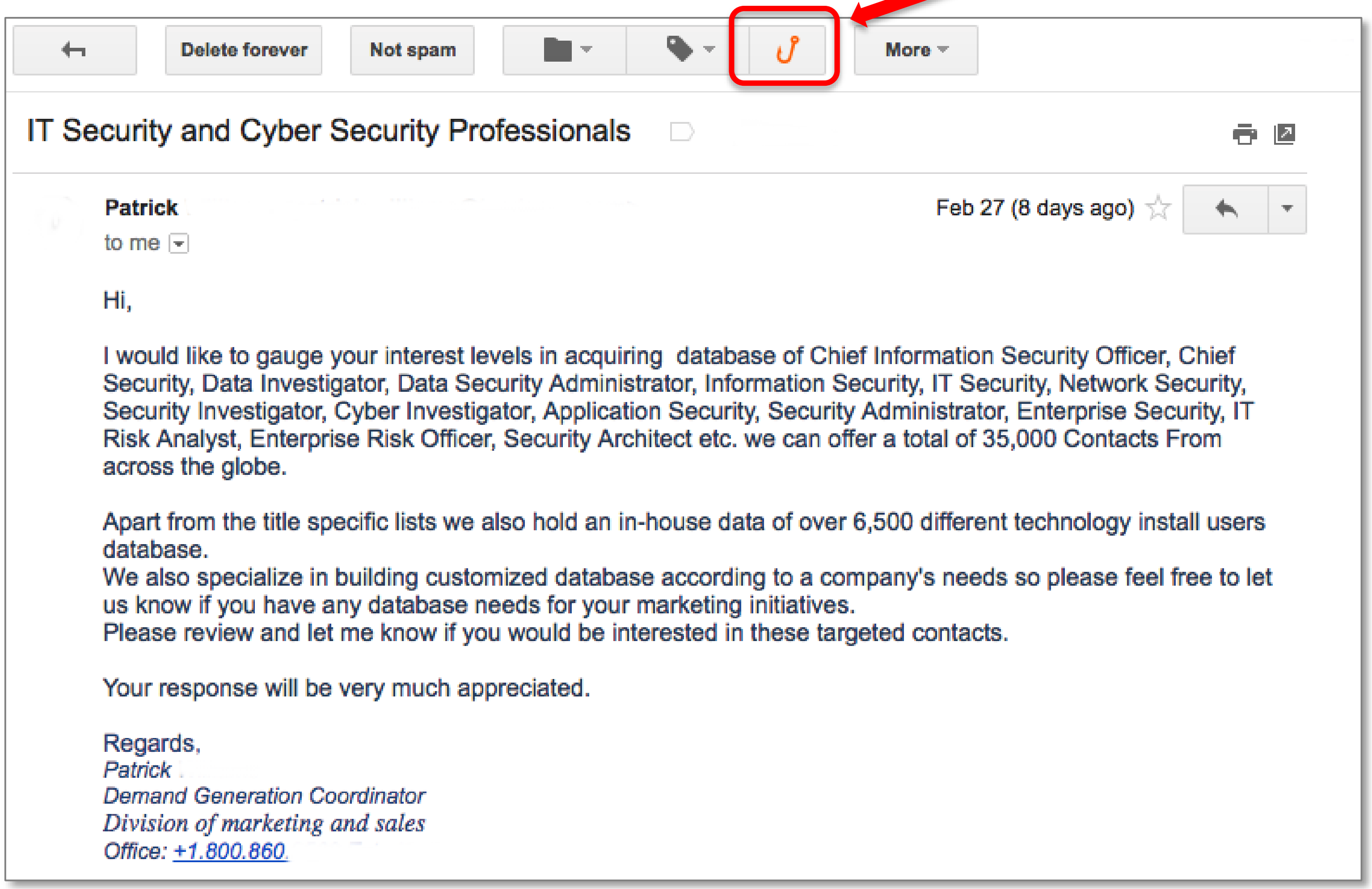
- I hover my mouse over a hyperlink that's displayed in the email message, but the **link to address is for a different website.** (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information** and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com - the "m" is really two characters – "r" & "n".

KnowBe4
Human error. Conquered.

Give Your Users An Action

- Give the users a way to provide the suspect email to someone that can review it

Free Phish Alert Button



IT Security and Cyber Security Professionals

Patrick
to me

Feb 27 (8 days ago)

Hi,

I would like to gauge your interest levels in acquiring database of Chief Information Security Officer, Chief Security, Data Investigator, Data Security Administrator, Information Security, IT Security, Network Security, Security Investigator, Cyber Investigator, Application Security, Security Administrator, Enterprise Security, IT Risk Analyst, Enterprise Risk Officer, Security Architect etc. we can offer a total of 35,000 Contacts From across the globe.

Apart from the title specific lists we also hold an in-house data of over 6,500 different technology install users database.
We also specialize in building customized database according to a company's needs so please feel free to let us know if you have any database needs for your marketing initiatives.
Please review and let me know if you would be interested in these targeted contacts.

Your response will be very much appreciated.

Regards,
Patrick
Demand Generation Coordinator
Division of marketing and sales
Office: +1.800.860

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

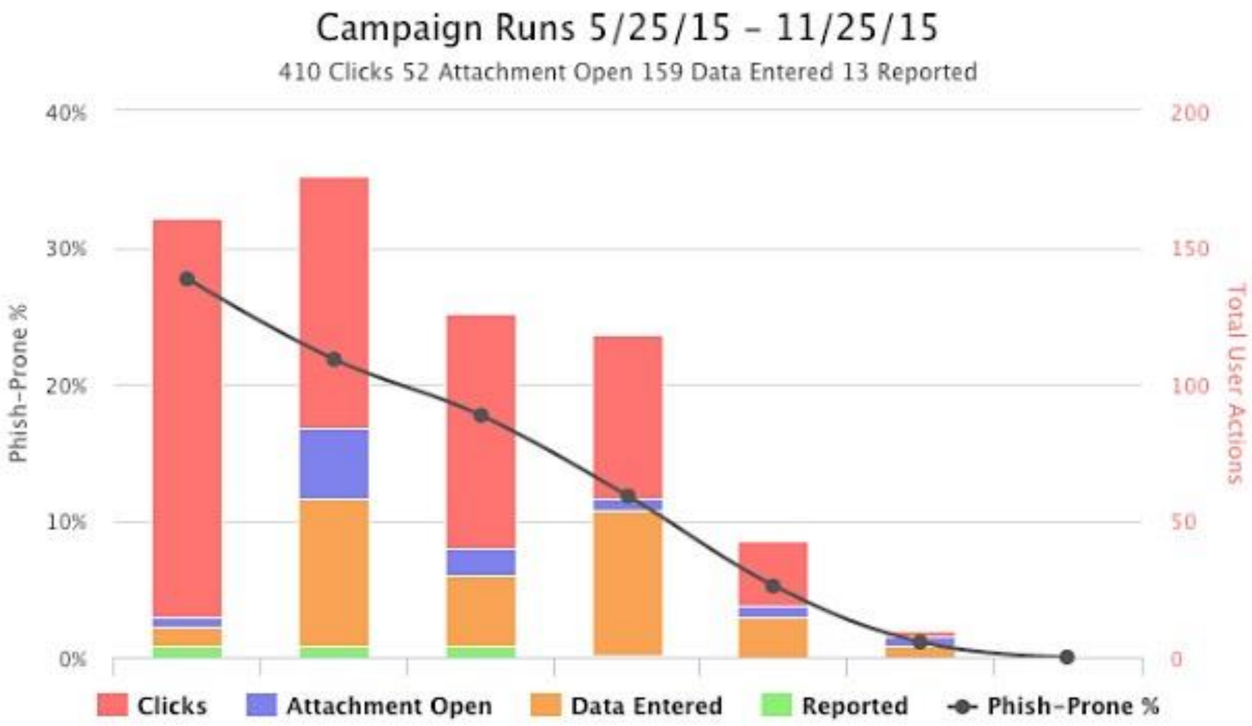
See The Results
Create reports showing stats and graphs for both training and phishing. Focus on areas of improvement

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

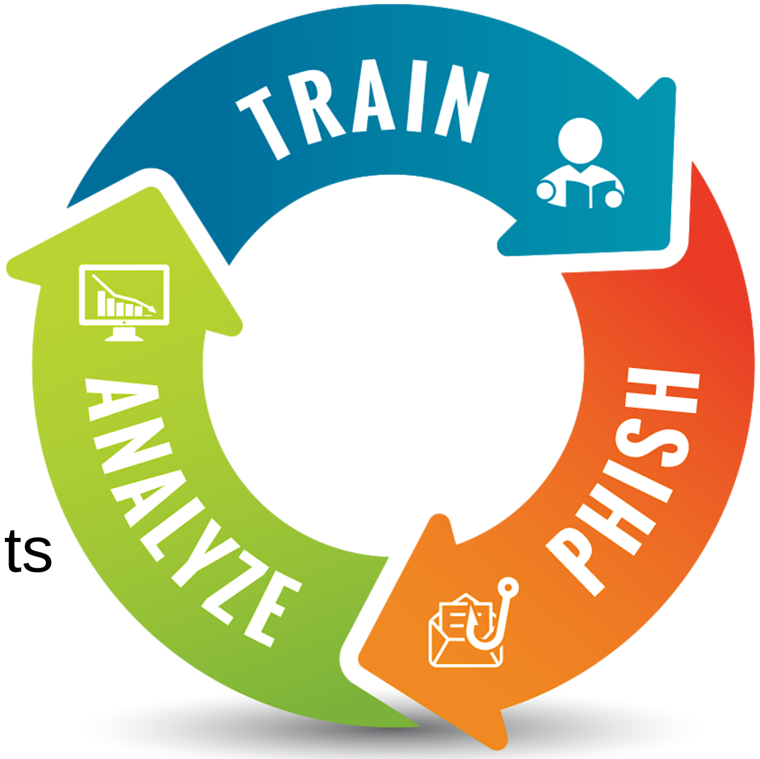
Continue to Test Employees Regularly

- 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

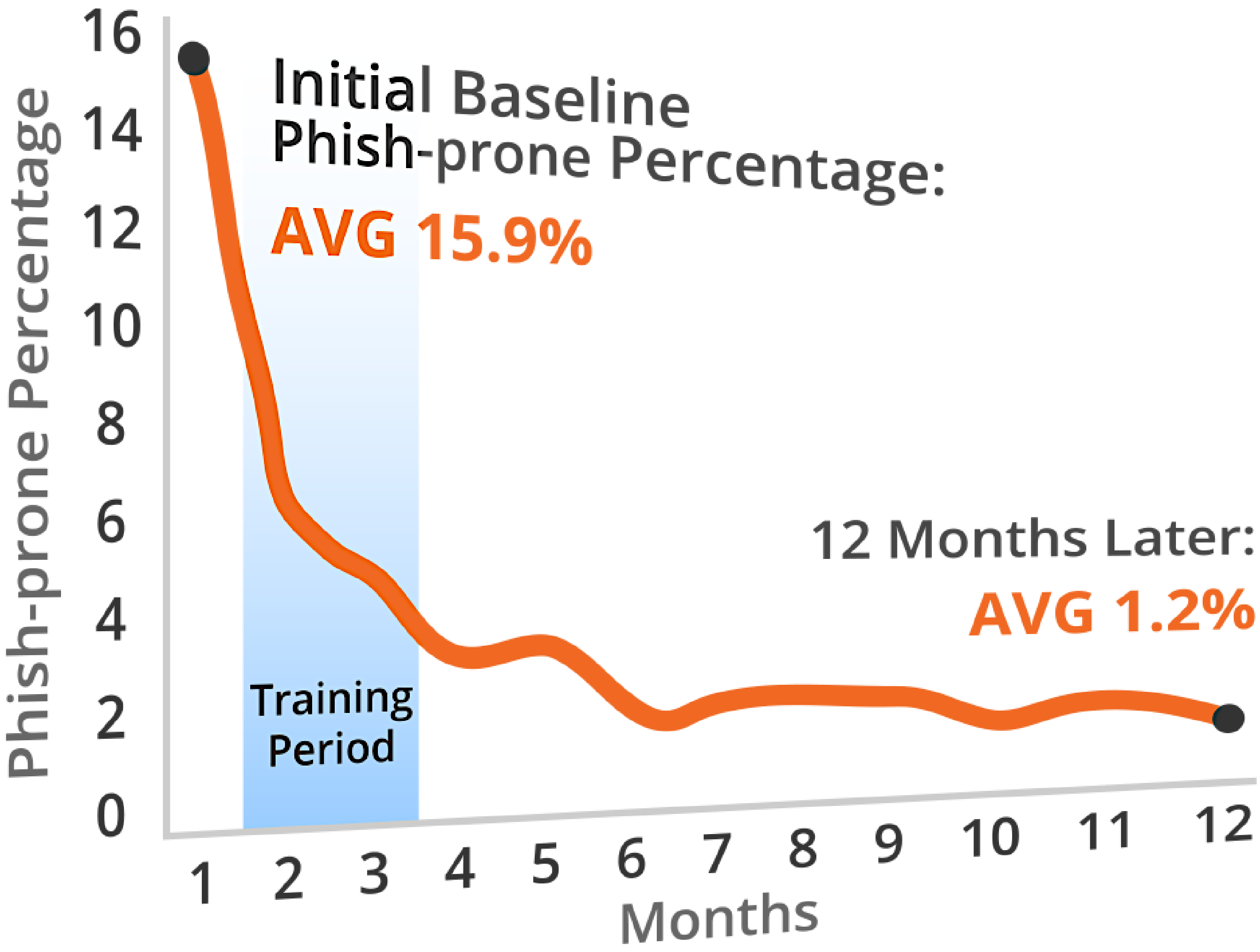
- The bad guys are always changing the rules, adjusting their tactics and upgrading their technologies

- 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!



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 «

Thank You!

Erich Kron – Security Awareness Advocate

Erichk@KnowBe4.com

@KB4Erich

www.madsqu1rrel.com

✉ Info@KnowBe4.com

🌐 www.KnowBe4.com

☎ 855-566-9234