KnowBe4
Human error. Conquered.

Top Threats

Roger A. Grimes
Data-Driven Security Evangelist
rogerg@knowbe4.com

Roger A. Grimes
Data-Driven Defense Evangelist
KnowBe4, Inc.

Twitter: @RogerAGrimes
LinkedIn: https://www.linkedin.com/in/rogeragrimes/

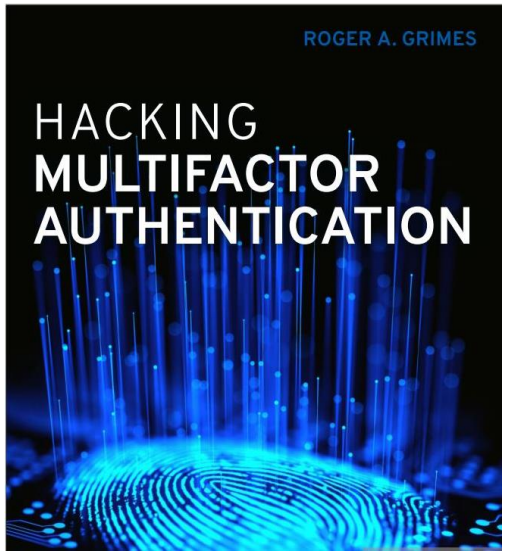
About Roger

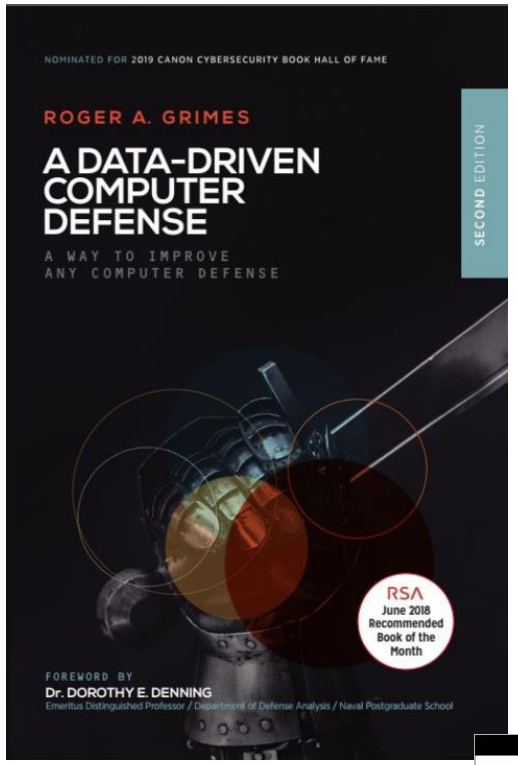
- 30 years plus in computer security
- Expertise in host and network security, IdM, crypto, PKI, APT, honeypot, cloud security
- Consultant to world's largest companies and militaries for decades
- Previous worked for Foundstone, McAfee, Microsoft
- Written 12 books and over 1,000 magazine articles
- *InfoWorld* and *CSO* weekly security columnist 2005 - 2019
- Frequently interviewed by magazines (e.g. Newsweek) and radio shows (e.g. NPR's All Things Considered)

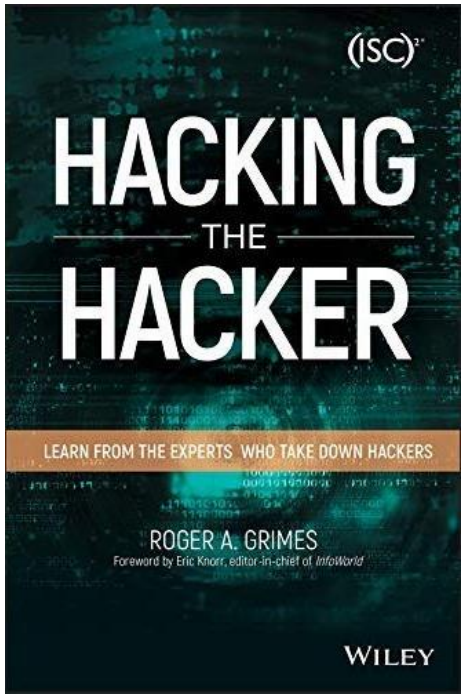
Certification exams passed include:

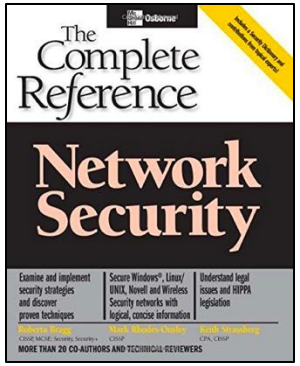
- CPA
- CISSP
- CISM, CISA
- MCSE: Security, MCP, MVP
- CEH, TISCA, Security+, CHFI
- yada, yada

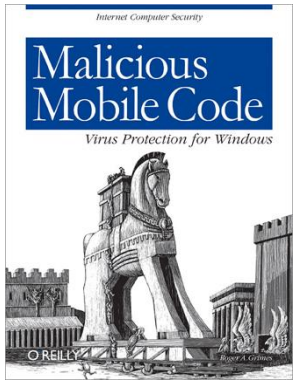
Roger's Books

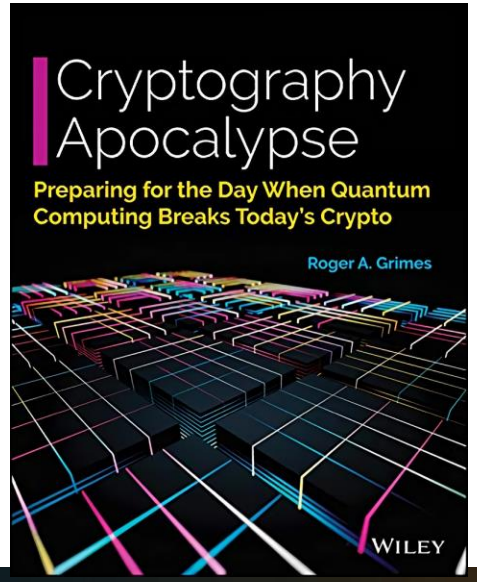


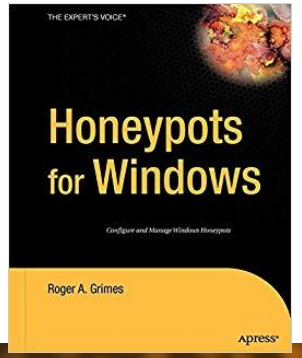


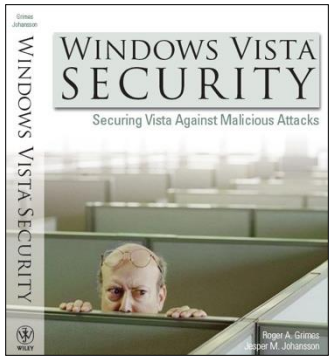


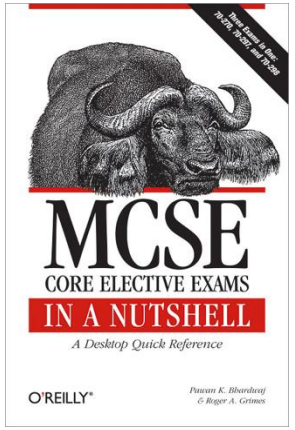


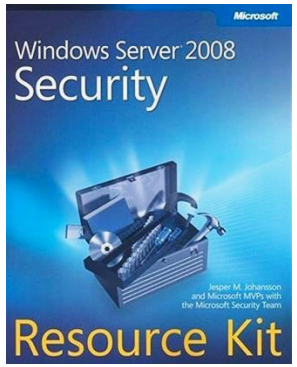






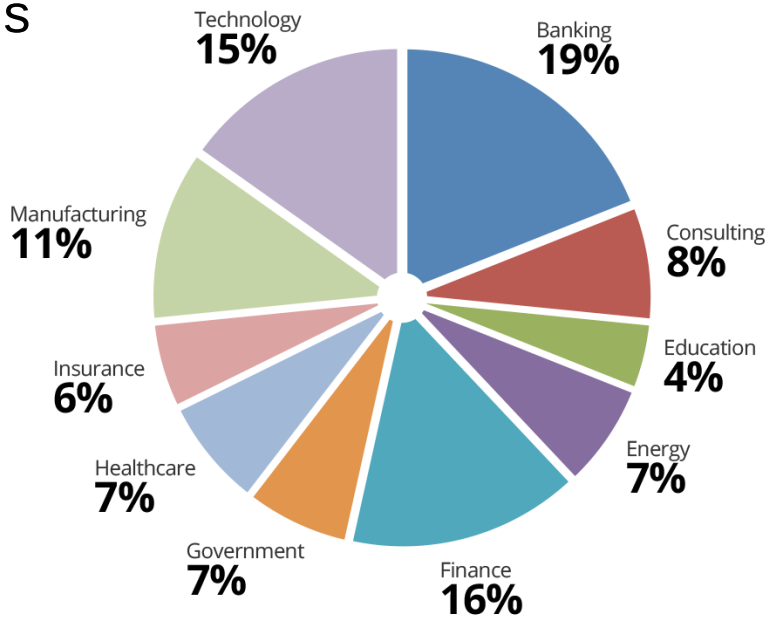






KnowBe4, Inc.

- 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
- We help tens of thousands of organizations manage the problem of social engineering



Why Hackers Hack

Your Org Was a:

- Victim of opportunity (random, malware involved)
- Targeted (human adversary involved from the start)

- Victims of opportunity attacks are far more common

- You can't as easily stop a targeted attack, but you can more easily put down opportunity attacks

More Malicious Ransomware

Summary - Nuclear Badness

- Steal Intellectual Property/Data
- Steal Credentials
- Threatening Victim's Employees and Customers
- Using Stolen Data to Spear Phish Partners and Customers
- Public Shaming

Good luck having a good backup save you!

More Malicious Ransomware

Steal/Leak Data

- Ransomware now FREQUENTLY copies data before encrypting it
- Determines company's "crown jewels"
- Target database servers, stop processes, copies GB of data
- Threatens to post publicly, give to victim's competitors
- Ransomware groups involved so far: Zeppelin, Maze, Revil/Sodinokibi, Snatch, etc.

More Malicious Ransomware

Steal/Leak Data

e encrypting it

e, Revil/Sodinokibi, Snatch,

CYBER / NEWS BRIEFS

Allied Universal Breached by Maze Ransomware, Stolen Data Leaked

22 Nov 2019 | OODA Analyst

Maze ransomware oper
that were allegedly sto
during the recent atta

January 14, 2020

Nemty ransomware makers may be latest to adopt data leak strategy

Sodinokibi Ransomware Publishes Stolen Data for the First Time

By Lawrence Abrams

January 11, 2020 06:07 PM 2

More Malicious Ransomware

Steal/Leak Data

- Ransomware now FREQUENTLY copies data before encrypting it

Boeing, Lockheed Martin, SpaceX Docs Leaked by Ransomware Gang

"The data was pilfered and dumped on the internet by the criminals behind the DoppelPaymer Windows ransomware, in retaliation for an unpaid extortion demand. The sensitive documents include details of Lockheed-Martin-designed military equipment—such as the specifications for an antenna in an anti-mortar defense system—according to a *Register* source who alerted us to the blueprints.

Other documents in the cache include billing and payment forms, supplier information, data analysis reports, and legal paperwork. There are also documents outlining SpaceX's manufacturing partner program."

More Malicious Ransomware

Steal Credentials

- Ransomware hackers search for every credential they can steal and re-use to maximize pressure, future pain, future financial gain
- Notpetya stole Windows/Active Directory credentials
  - But only to propagate
- Ransomware gangs now extract every found credential they can before revealing themselves and asking for ransom
- They don't usually tell you they have done it

More Malicious Ransomware

Steal Credentials

Example:

- Ransomware hackers were
- Used Trickbot trojan to colle

Indeed, Holden shared records of communications from VCPI's tormentors suggesting they'd unleashed Trickbot to steal passwords from infected VCPI endpoints that the company used to log in at *more than 300 Web sites and services*, including:

-Identity and password management platforms Autho and LastPass
-Multiple personal and business banking portals;
-Microsoft Office365 accounts
-Direct deposit and Medicaid billing portals
-Cloud-based health insurance management portals
-Numerous online payment processing services
-Cloud-based payroll management services
-Prescription management services
-Commercial phone, Internet and power services
-Medical supply services
-State and local government competitive bidding portals
-Online content distribution networks
-Shipping and postage accounts
-Amazon, Facebook, LinkedIn, Microsoft, Twitter accounts

More Malicious Ransomware

Threaten Victim's Employees

- Ransomware now targets employees of victim
- Notifies employees that they have the employee's logon credentials, SSN, personal info, etc.

More Malicious Ransomware

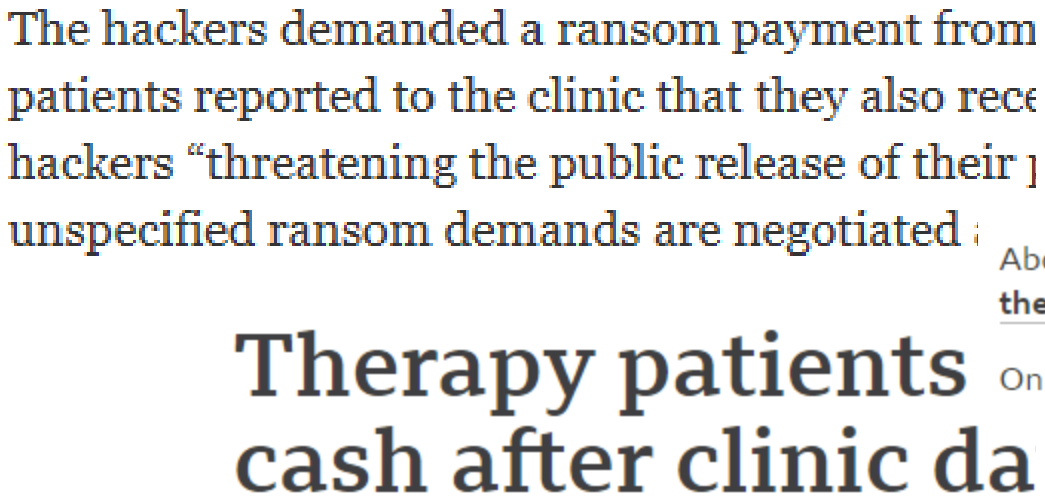
Threaten Victim's Customers

- Let's the victim's customers know that they have their logons and private data and will release publicly
- Sometimes actually extort the customer in addition to the company

More Malicious Ransomware

Threaten Victim's Customers

- Ransomware gang says PATIENTS of a compromised plastic surgery center must pay or else they will go public



The hackers demanded a ransom payment from
patients reported to the clinic that they also rece
hackers "threatening the public release of their
unspecified ransom demands are negotiated

Therapy patients
cash after clinic da

'Extremely uncomfortable'

Jere - who asked for his surname not be published - told BBC News someone calling themselves "the ransom guy" had told him:

- Vastaamo had refused to pay 40 bitcoin (£403,000)

About 300 records have already been published on the dark web, **according to the Associated Press news agency**.

On its website, the clinic calls the attack "a great crisis".

"I'm anxious about the fact that the attackers are in possession of my notes and conversations from those psychiatrist sessions," Jere said.

"Those notes contain things I'm not ready to share with the world.

More Malicious Ransomware

Threaten Everyone – Real-World Example

Because of Robert Denison failed to take very simple security measures on his devices, I hacked into all employees google accounts that were hosted under the domain name of denisonyachtsales.com

All company leads, accounting archives, employee social security numbers, employee signatures including the data that sent from "clients" of Denison Yachting to the mailing accounts of the company is under my control.

So if you ever conducted business with Bob Denison, your private data might be in my hands right now.

What do I ask for?

I want Bob to send 15 BTC to this Bitcoin wallet address; 3J7sKP8dmoyisj2dcJoExfBUuvE5pPP9nT

What will happen if my demand won't be fulfilled? When the countdown here finishes, all the data that mentioned previously will be publicly available for anyone who visits this webpage.

Bob, this was your fault, don't make other people pay for your fault. For any questions, reach me at denisonextortion@protonmail.com

If this website shuts down, you can track the countdown on denisonextortion.com

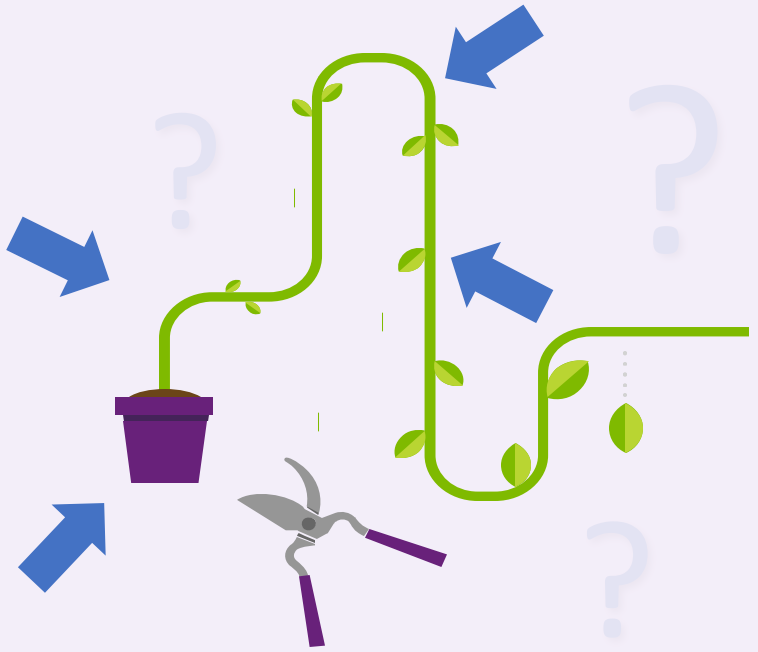
0d 18h 11m 51s

Root Causes of Cybersecurity Incidents

root causes → how attackers/malware break in

What's the number one root cause threat in your environment?

- Programming Bug (patch available or not available)
- Social Engineering
- Authentication Attack
- Human Error/Misconfiguration
- Eavesdropping/MitM
- Data/Network Traffic Malformation
- Insider Attack
- 3rd Party Reliance Issue (vendor/dependency/watering hole)
- Physical Attack
- Brand New Attack Vector (w/o current/default mitigation)



Ask Yourself 3 Key Questions:

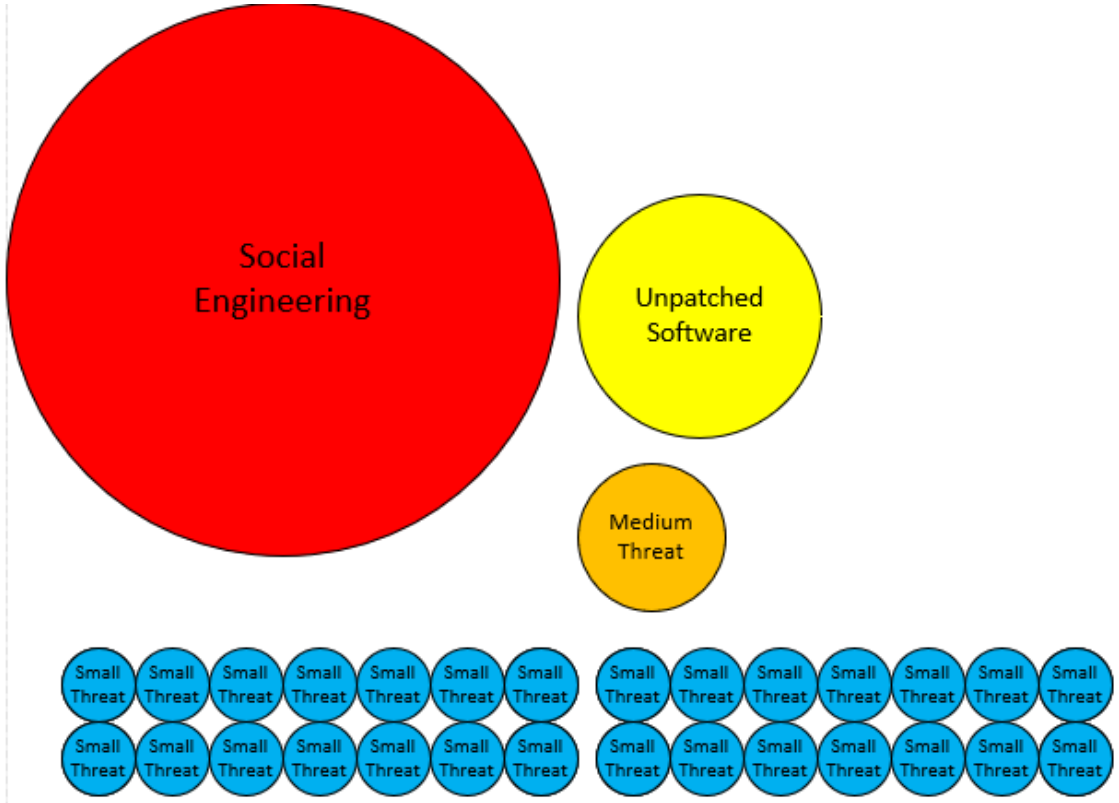
1. Can your team correctly answer what is the top root cause?
2. Is the answer consistent across all stakeholders?
3. Do you have data to back up the right answer?

Biggest Initial Breach Root Causes for Most Companies

- Social Engineering
- Unpatched Software

- But don't trust me,

  measure your own risk

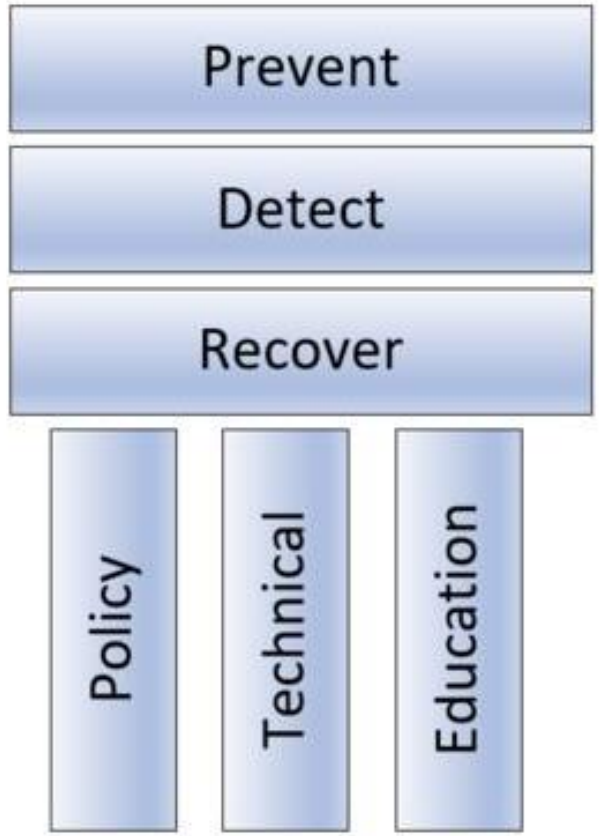


Social engineering is responsible for 70% - 90% of all malicious data breaches

https://blog.knowbe4.com/70-to-90-of-all-malicious-breaches-are-due-to-social-engineering-and-phishing-attacks

3 x 3 Security Control Pillars

For every high-risk threat you want to mitigate, create 3 x 3 controls



3 x 3 Security Control Pillars - https://www.linkedin.com/pulse/3-x-security-control-pillars-roger-grimes

Best Defenses

Top Defenses for Most Organizations

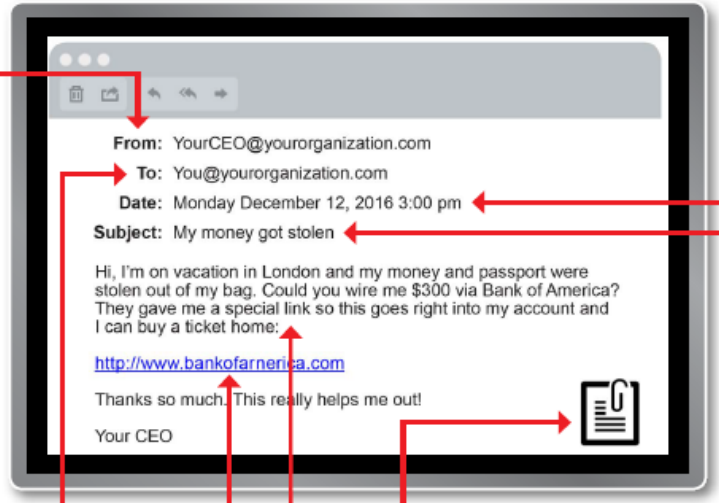
(in order of importance)

- **Mitigate Social Engineering**
- **Patch Internet-accessible software**
- **Use non-guessable passwords/multi-factor authentication**
  - Different passwords for every website and service
- **Teach Users How to Spot Rogue URLs**
  - https://blog.knowbe4.com/top-12-most-common-rogue-url-tricks
  - https://info.knowbe4.com/rogue-urls
- **Use Least-Permissive Permissions**
- **Run OSINT tools on your org to learn what is out there**

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 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** 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**?

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, 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.

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.

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" and "n."

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?

KnowBe4
Human error. Conquered.

THE RED FLAGS OF ROGUE URLs

Spotting malicious URLs is a bit of an art. The examples represented here are some of the common tricks used by hackers and phishers to fool users to visiting malicious websites. The methods shown here could be used by legitimate services, but if you see one of these "tricks" you need to make sure you're dealing with the organization you think you are.

Look-a-Alike Domains

Domain names which **seem** to belong to respected, trusted brands.

Slight Misspellings

Microsoftnline
<v5pz@onmicrosoft.com>

www.llnkedin.com

Brand name in URL, but not real brand domain

ee.microsoft.co.login-update-dec20.info

www.paypal.com.bank/logon?user=johnsmith@gmail.com

ww17.googlechromeupdates.com/

Brand name in email address but doesn't match brand domain

Bank of America
<BankofAmerica@customerloyalty.accounts.com>

Brand name is in URL but not part of the domain name

devopsnw.com/login.microsoftonline.com?userid=johnsmith

URL Domain Name Encoding

https://%77%77%77.%6B%6E%6F%77%62%654.%63%6F%6D

Shortened URLs

When clicking on a **shortened URL**, watch out for malicious redirection.

https://bit.ly/2SnA7Fnm

Domain Mismatches

Human Services .gov
<Despina.Orrantia6731610@gmx.com>

https://www.le-blog-qui-assure.com/

Strange Originating Domains

MAERSK
<info@onlinealxex.com.pl>

Overly Long URLs

URLs with 100 or more characters in order to **obscure the true domain**.

http://innocentwebsite.com/irs.gov/logon/fasdjkg-sajdkjndf
jnbkasldjfbkajsdbfkjbasdf/adsnfjksdngkfdfgfgjhfgd/ght.php

File Attachment is an Image/Link

It looks like a file attachment, but is really an **image file with a malicious URL**.

PDF INV39391.pdf
52 KB

https://d.pr/free/f/jsaeoc
Click or tap to follow link.

Open Redirectors

URLs which have hidden links to completely different web sites at the end.

t-info.mail.**adobe.com**/r/?id=hc347a&p1=**evilwebsite.com**

KnowBe4

The KnowBe4 Security Awareness Program WORKS

Baseline Testing
Use simulated phishing to baseline assess the Phish-prone™ percentage of your users.

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.

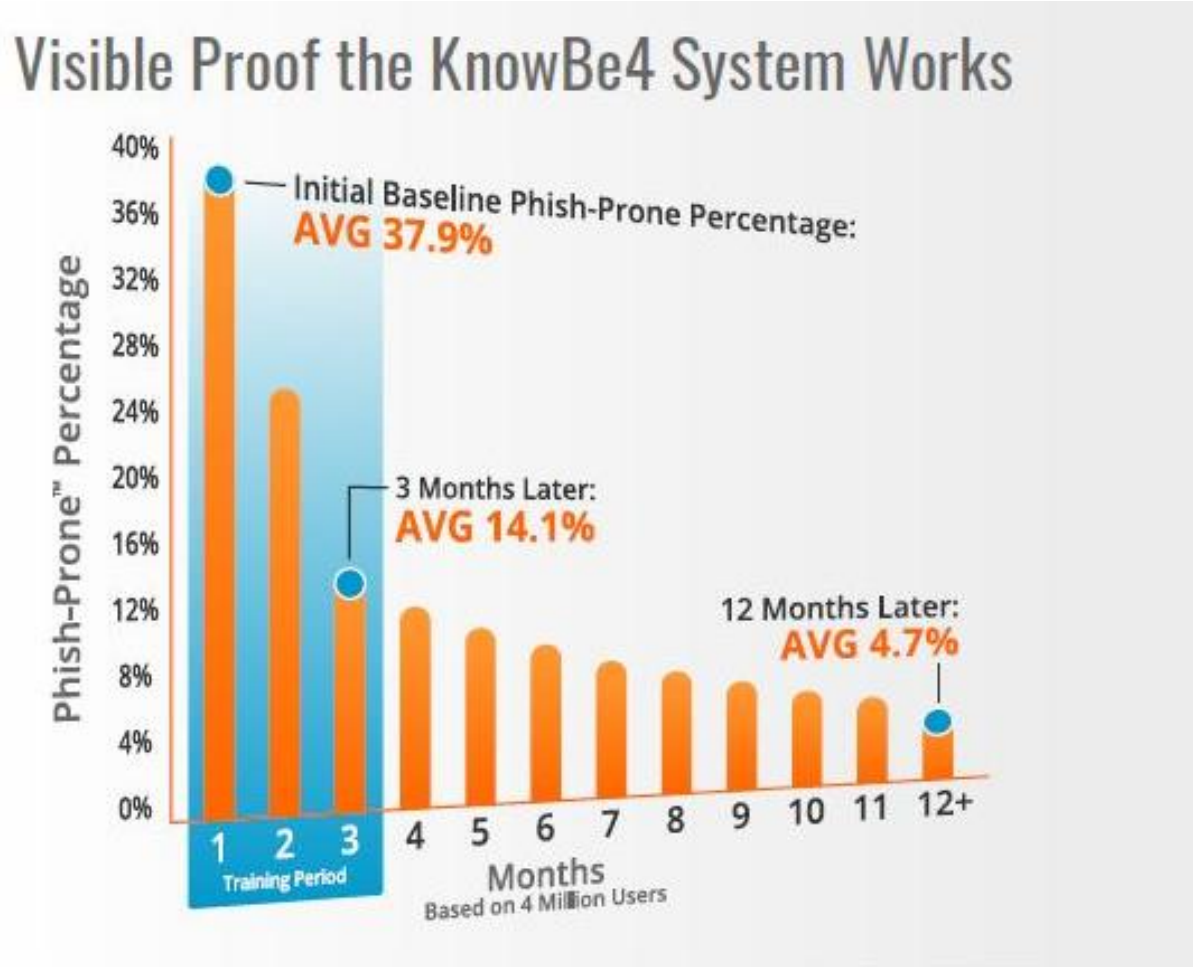
See the Results
Enterprise-strength reporting, showing stats and graphs for both training and phishing, ready for management. Show the great ROI!

Security Awareness Training Program That Works

- Drawn from a data set of **over four million users**
- Over **17K organizations**
- **Over 9.1M** Simulated Phishing Campaigns

- Segmented **by industry type** and **organization size**

https://info.knowbe4.com/phishing-by-industry-benchmarking-report



Questions?

Roger A. Grimes– Data-Driven Defense Evangelist, KnowBe4
rogerg@knowbe4.com
Twitter: @rogeragrimes
https://www.linkedin.com/in/rogeragrimes/