KnowBe4
Human error. Conquered.

Now That Ransomware Has Gone Nuclear, How Can You Avoid Becoming the Next Victim?

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/

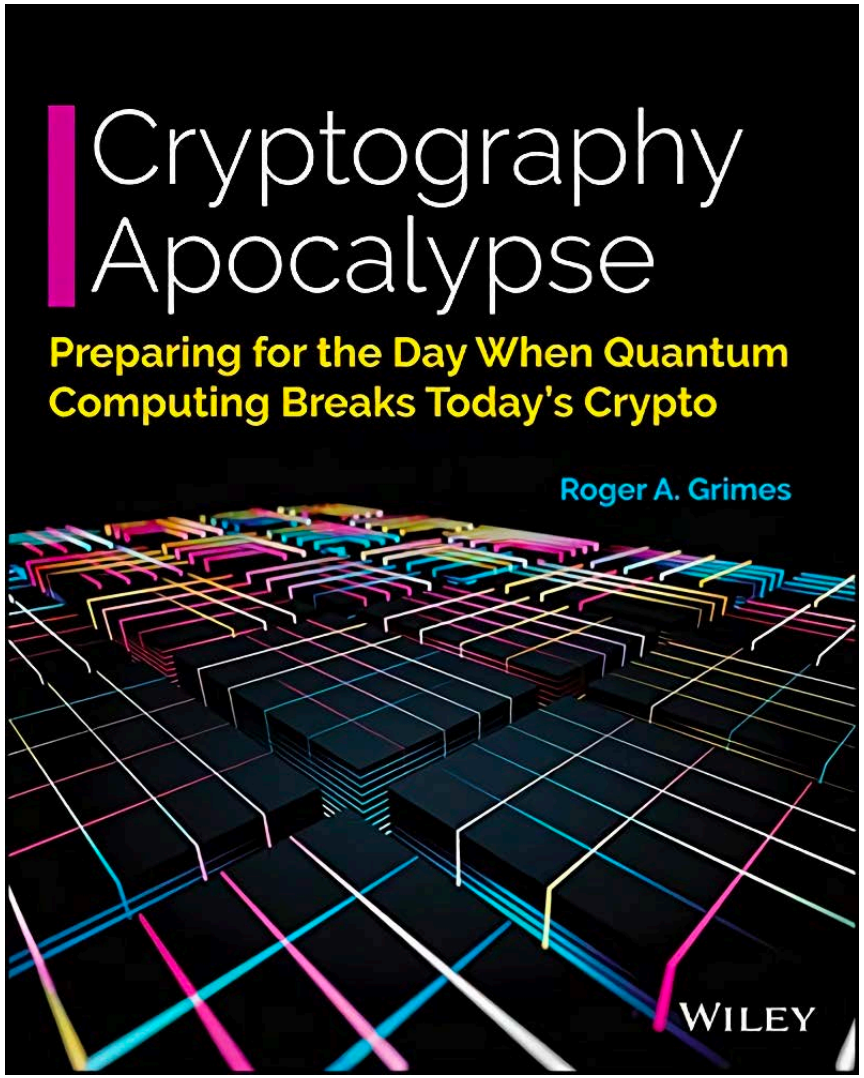
About Roger

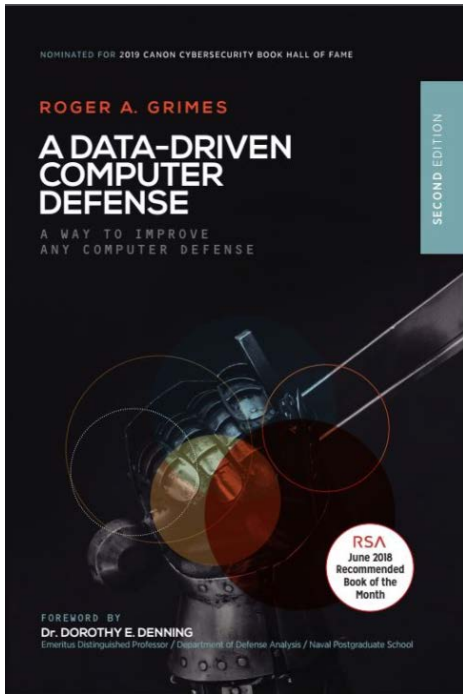
- 30 years plus in computer security
- Expertise in host and network security, IdM, crypto, PKI, APT, honeypot, cloud security
- Consultant to world's largest companies and militaries for decades
- Previous worked for Foundstone, McAfee, Microsoft
- Written 11 books and over 1,000 magazine articles
- *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)

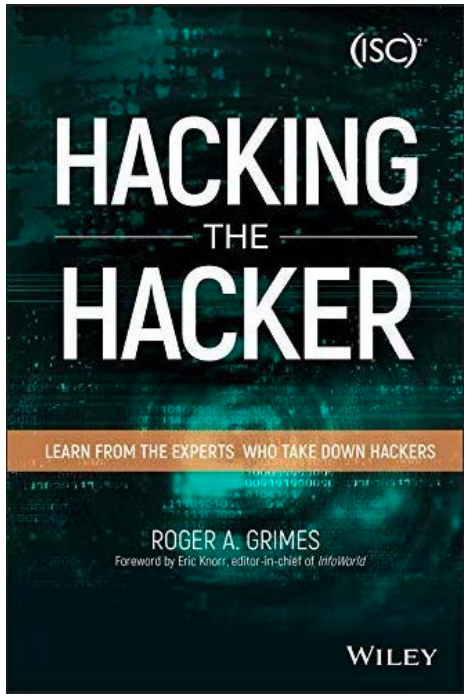
Certification exams passed include:

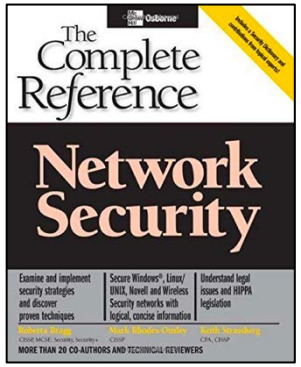
- CPA
- CISSP
- CISM, CISA
- MCSE: Security, MCP, MVP
- CEH, TISCA, Security+, CHFI
- yada, yada

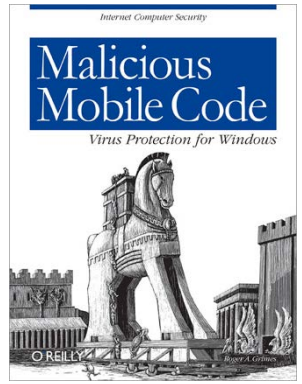
Roger's Books

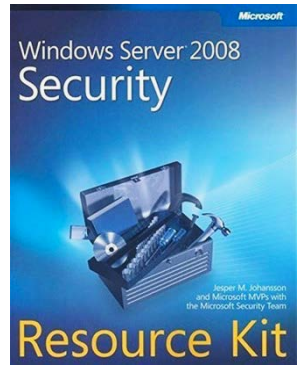


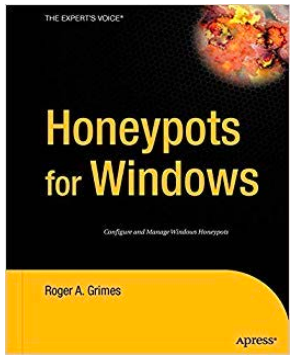


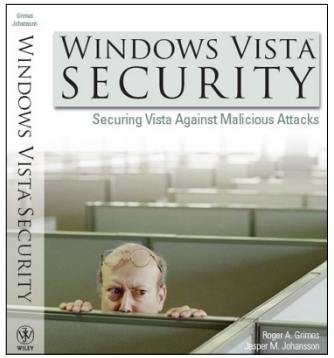


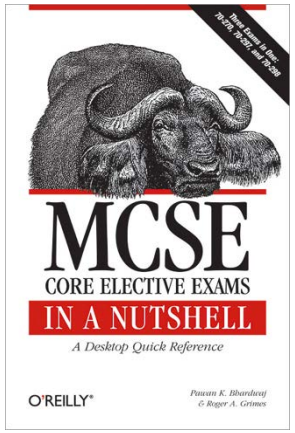






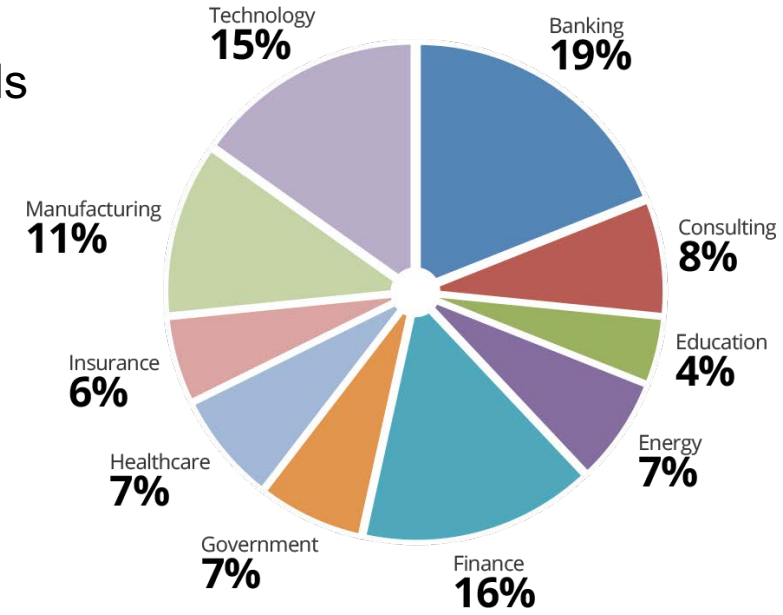






KnowBe4, Inc.

- 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
- 200% growth year over year
- We help tens of thousands of organizations manage the problem of social engineering



Agenda

- Traditional Ransomware
- How Ransomware Is Becoming More Malicious
- Defenses

Agenda

- Traditional Ransomware
- How Ransomware Is Becoming More Malicious
- Defenses

Ransomware Basics

History of Ransomware

- 1989 - First ransomware program was the AIDS Cop trojan
- 2005 – First contemporary ransomware programs began to show up, using asymmetric encryption
- 2013 – CryptoLocker asks for bitcoin payment
- 2016 – Samsam attacks using RDP bruteforce password guessing
- 2017 – Petya attacks Ukraine
- 2017 – Notpetya attacks Maersk causing $300M in damages
- 2017 – Wannacry - $300 ransom had to be paid in 7 days or files deleted
  - Used 20 localized languages

Ransomware Basics

Popular Ransomware

- Wannacry
- GandCrab
- GlobalImposter
- Phobos
- Cerber
- Jaff
- Spora

Ransomware Basics

Ransomware Destruction Maturity over Years

- **Early**: Used to encrypt immediately upon executing, didn't care where it was
- **Middle**: Spread like a worm, then encrypted
- **Contemporary**: Break in, dial-home and notify hacker, so they can figure out best strategy, and then hacker:
  - Determines what to encrypt to get the best bang for the buck
  - Determines what to encrypt to make victim go uncle fastest
  - Determines ability of victim to pay how much
  - Disables/corrupts online backups
  - Disables/corrupts offline backups
- Now…

Ransomware Basics

Ransomware Getting More Sophisticated

- Simply in victim's environment much longer, doing analysis and research
- Ransomware-as-a-Service (RaaS)
  - Updates go out to all their customers and victims ASAP
- Using built-in, trusted tools (e.g. Powershell) to do maliciousness
- Maliciously encrypting your data backups with keys you don't know
- So you think you have great backups, but you really don't

Ransomware Basics

Ransomware Response Maturity over Years

- **Early**: Victims Usually Didn't Pay
- **Middle**: Insurance Arriving on Scene/Victims More Likely Pay
- **Contemporary**: Victims Almost Always Pay (even if they say they don't do)

  Typical Scenario:
  - Victim calls insurance company
  - Insurance co. calls incident response broker that specializes in ransomware attacks
  - Broker calls all the needed specialists, has all the needed relationships
  - Stop the damage specialists
  - Recovery specialists
  - Professional, full-time, negotiators handle the ransom payment (amount to pay, etc.)
  - Media response teams

Agenda

- Traditional Ransomware
- How Ransomware Is Becoming More Malicious
- Defenses

More Malicious Ransomware

Essentially:

- Ransomware crooks got tired of victims saying no
- They realized the access they had was “gold” and that they could do anything
- Encrypting data and holding it for hostage was the least of the victims worries now…

More Malicious Ransomware

Summary - Nuclear Badness

- Steal Credentials
- Public Shaming
- Steal Intellectual Property/Leak Data
- Threatening Victim's Customers

Good luck having a good backup save you!

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

- Ransomware hackers were in company for 14 months without detection
- 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

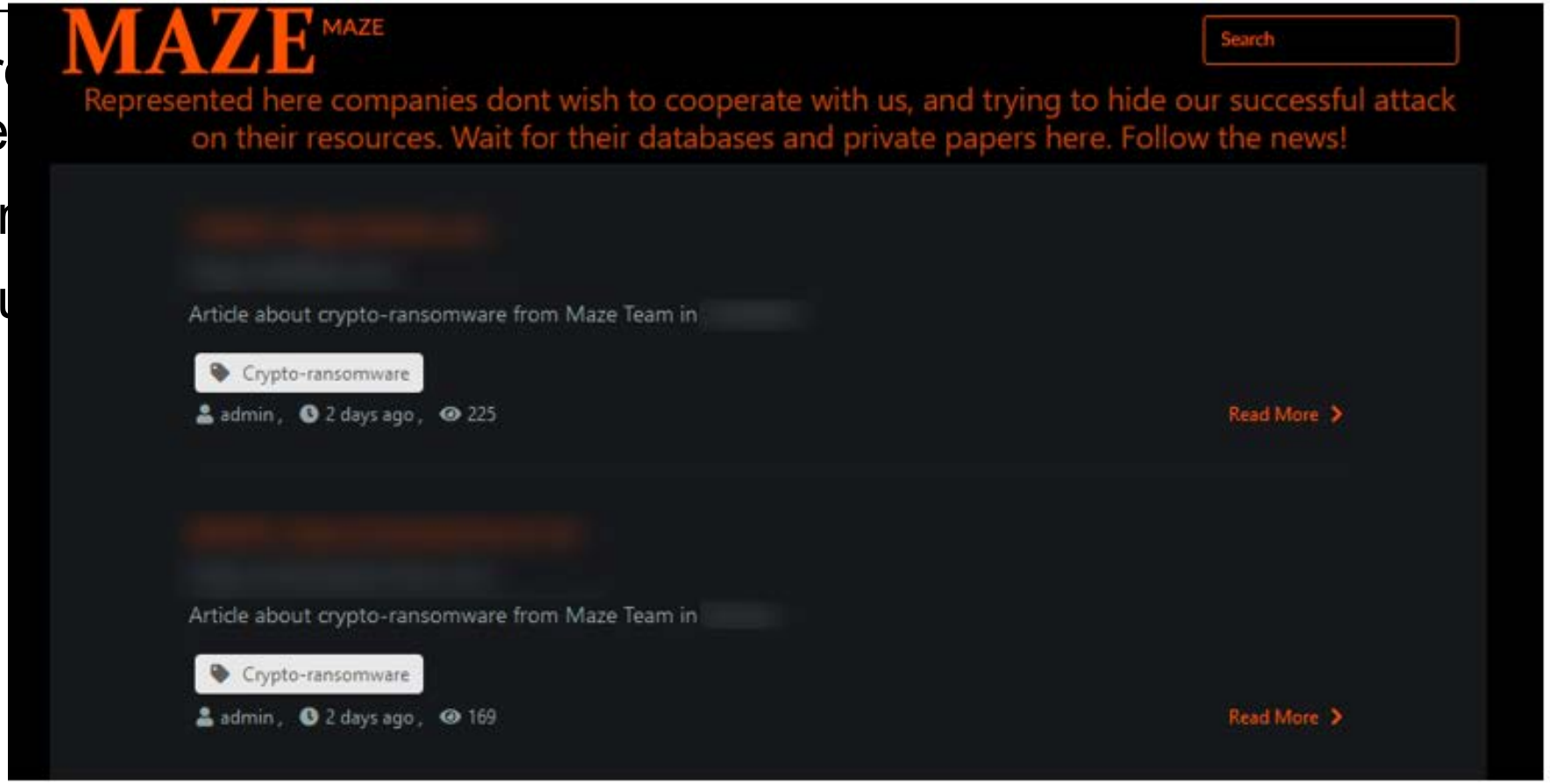
Public Shaming

- Ransomware will threaten to reveal publicly that you and your data has been compromised
- Maze ransomware group is one of the first to do this
- Created a public website/blog to display the names of companies they exploited
- List victim names
- Discuss data stolen
- Contact media sites to spread the news

More Malicious Ransomware

Public Shaming

- Ransomwar
- Maze ranso
- Created a pu



More Malicious Ransomware

Steal/Leak Data

- Ransomware now FREQUENTLY copies data before encrypting it
- Determine company's "crown jewels"
- Target database servers, stop processes, copy data
- Ransomware groups involved so far: Zeppelin, Maze, Revil/Sodinokibi, Snatch, etc.

More Malicious Ransomware

Steal/Leak Data

encrypting it

, Revil/Sodinokibi, Snatch,

More Malicious Ransomware

Steal/Leak Data

Example: Travelex Ransomware attack

- Hackers broken in using missing server VPN patches (that were patched last year)
- $6M ransom
  - When Travelex first refused, ransom was $3M, then hacker revealed he had customer data and wanted $6M
- Sodinokibi REvil ransomware gang
- In for 6 months
- 5GB of sensitive customer data including SSN, DOB, CC, etc.
- Hackers gave 7 days to respond
- Travelex down at least 18 days

More Malicious Ransomware

Threaten Victim's Customers

- Ransomware now targets MSSP (Managed Security Service Providers) and their customers
- They compromise MSSP and then compromise all their customers at once, hitting each customer individually, or:
- They do the same but tell the MSSP to pay up or they will compromise their customers
  - So, if MSSP pays big, none of the MSSP's customers will ever know, unless the MSSP self-reports

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 with what plastic surgery each patient had.

> The hackers demanded a ransom payment from Davis and by November 29, about 15 to 20 patients reported to the clinic that they also received individual extortion attempts from the hackers "threatening the public release of their photos and personal information unless unspecified ransom demands are negotiated and met."

More Malicious Ransomware

Future

- It's just going to get worse!

- This is just the middle!

Agenda

- Traditional Ransomware
- How Ransomware Is Becoming More Malicious
- Defenses

Defenses

What The Real Problem Really Is

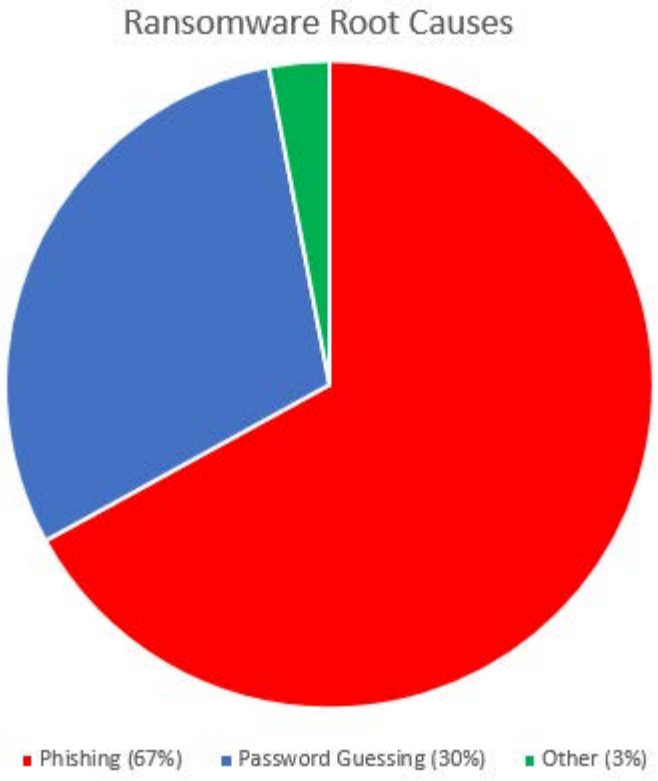
- Ransomware is not the real problem
- It's how ransomware got in
- It's how ransomware got admin

- If you don't stop hackers and malware from breaking in and getting admin you're never going to stop the nuclear badness
- They will always be able to do very bad things

Defenses

Top 3 Defenses For My Money

- Focus on security awareness training
- Focus on better patching
- Focus on credential hygiene/MFA



Defenses

- Regular, defense-in-depth, computer defenses
- Total, tested restore of backup of critical systems
- Elevated credential protection/hygiene/monitoring
- Change all possible passwords and not just internal network passwords after a ransomware compromise
- DLP tools
- Network traffic anomaly analysis
- Encrypt data so that you can disable it's viewing remotely
  - Ex. Active Directory Rights Management Service
- Cyber insurance
- Media incident response team

Defenses

- Communicate how ransomware is changing and how a backup will not save you to your computer security team and management
  - Use this slide deck as part of your security awareness training

The KnowBe4 Security Awareness Program WORKS

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

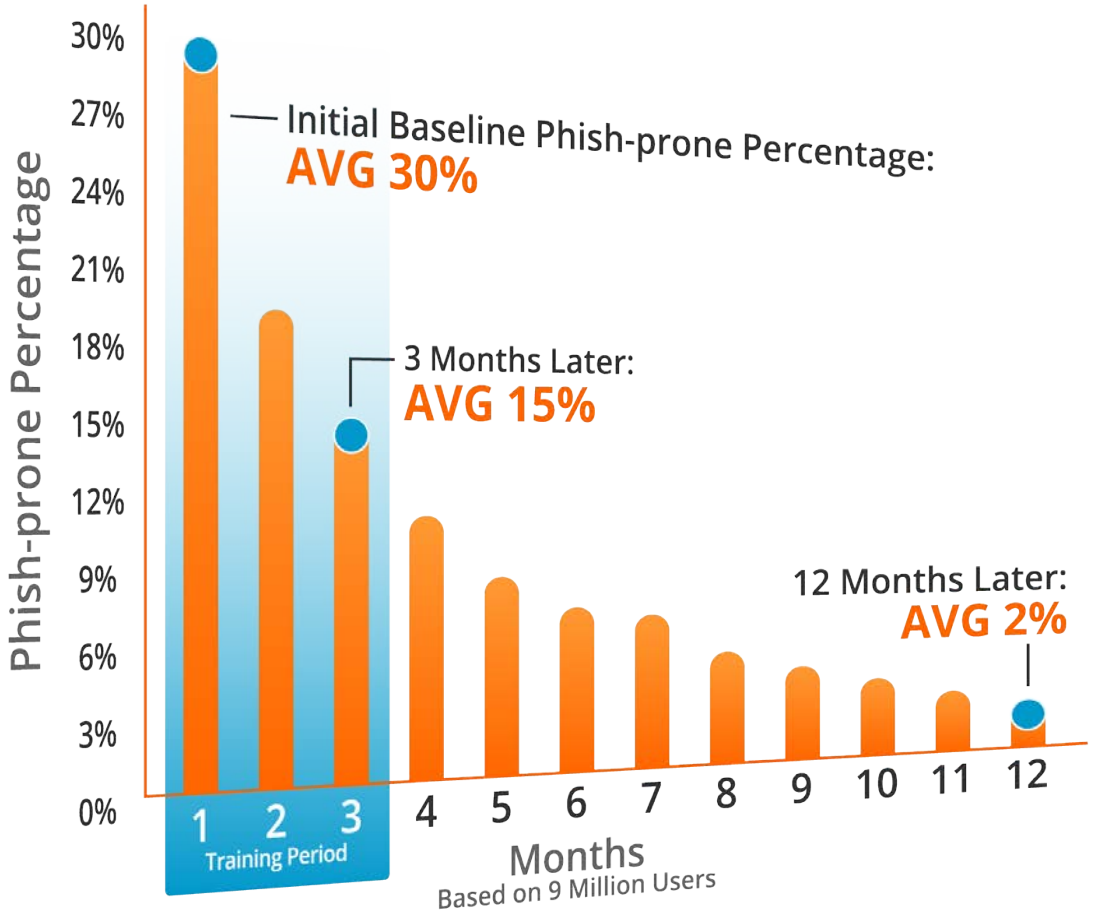
Train Your Users
The world's largest library of security awareness training content; including interactive modules, videos, games, posters and newsletters. Automated training campaigns with scheduled reminder emails.

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 six million users**
- Across **nearly 11K organizations**
- Segmented **by industry type** and **organization size**
- **241,762** Phishing Security Tests (PSTs)

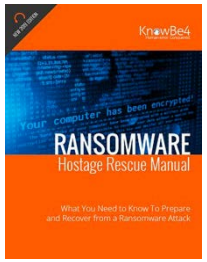


Resources

Free IT Security Tools

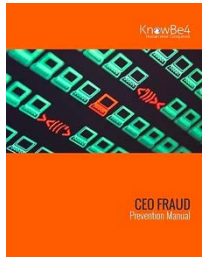
- Domain Doppelgänger
- Awareness Program Builder
- Domain Spoof Tool
- Mailserver Security Assessment
- Phish Alert
- Ransomware Simulator
- Weak Password Test
- Phishing Security Test
- Second Chance
- Email Exposure Check Pro
- Training Preview
- Breached Password Test

Whitepapers



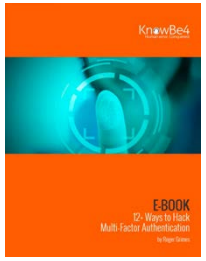
Ransomware Hostage Rescue Manual

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.



CEO Fraud Prevention Manual

CEO fraud is responsible for over $3 billion in losses. Don't be next. The CEO Fraud Prevention 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.



12+ Ways to Hack Two-Factor Authentication

All multi-factor authentication (MFA) mechanisms can be compromised, and in some cases, it's as simple as sending a traditional phishing email. Want to know how to defend against MFA hacks? This whitepaper covers over a dozen different ways to hack various types of MFA and how to defend against those attacks.

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

Questions?

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