YOUR PHISHING PROGRAM IS A WASTE OF TIME AND MONEY

Snake Oil? Summit 2023

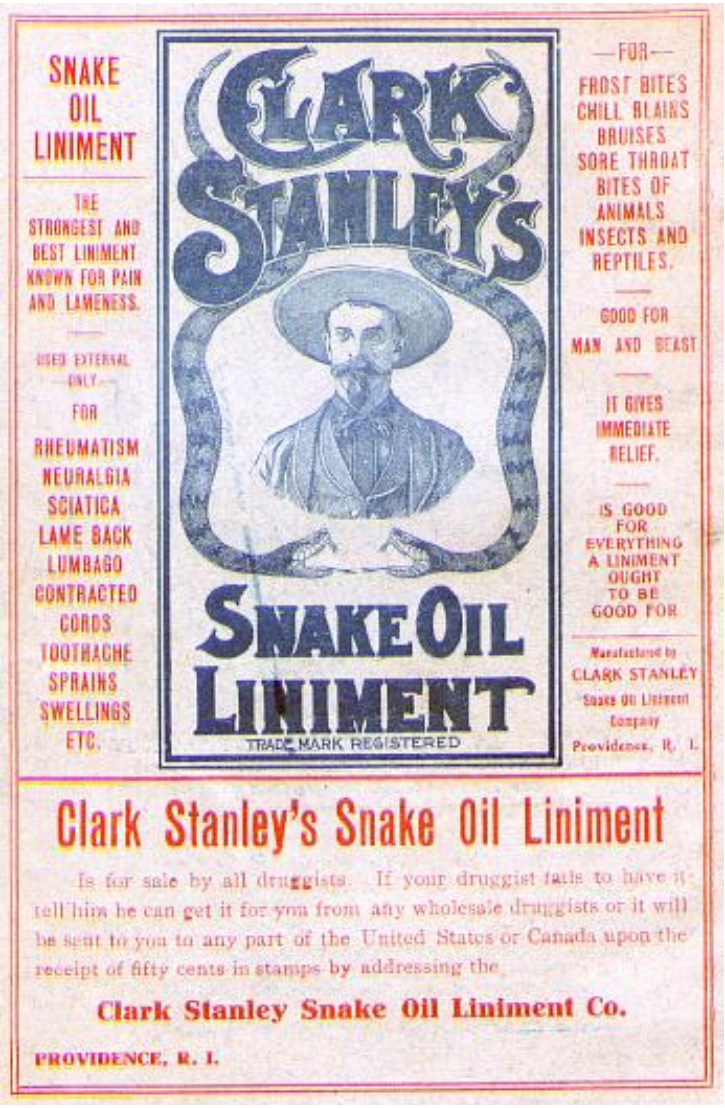
DISCLAIMER

I have intentionally left out any vendor references, as this is not a problem with a specific tool.

My beef is with the industry, or better yet, the subset of the industry that has let a checkbox compliance measure and vanity metrics derail many (most?) security programs.

AGENDA

- Current “Truth” in the Industry
- What does the data say?
- Snake Oil?
- Where to go from here?

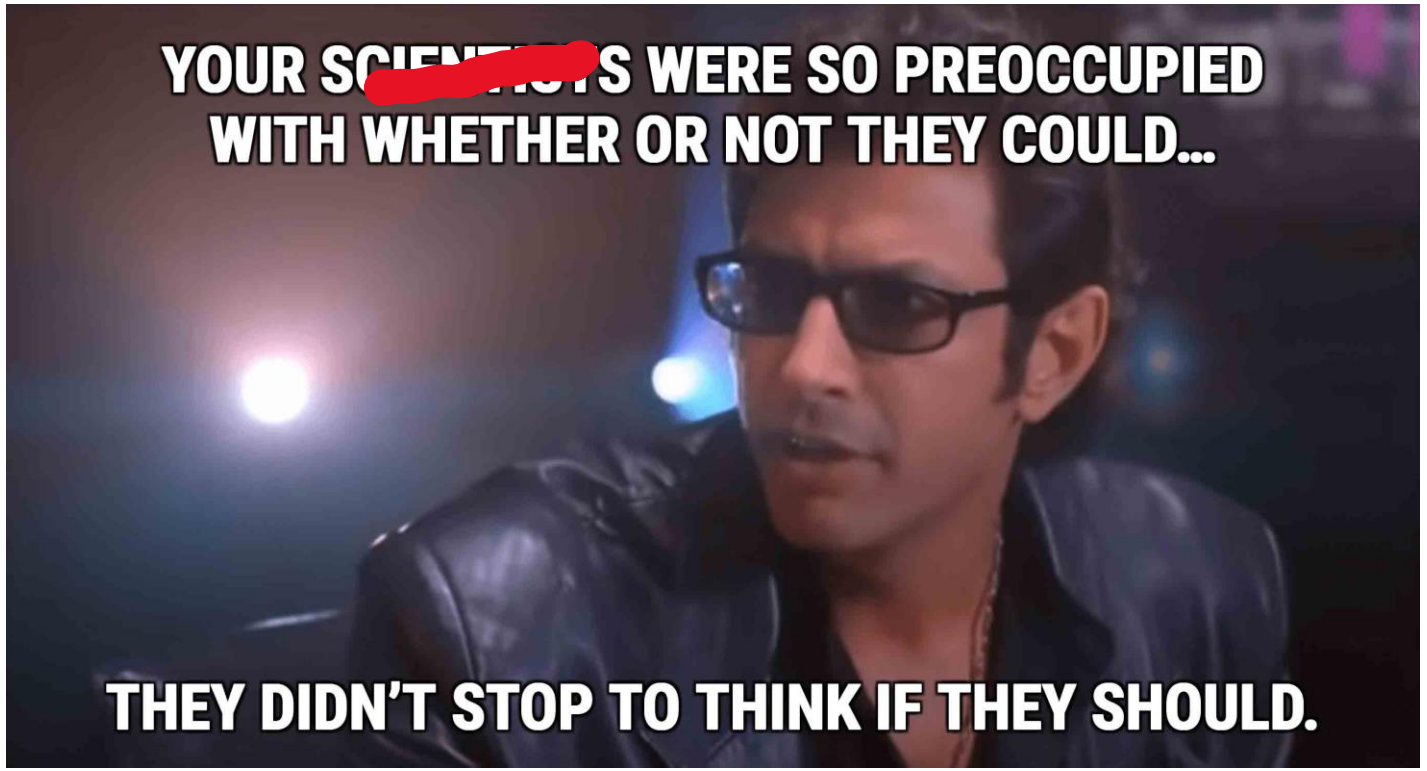


INDUSTRY “TRUTHS”

Simulating phishing is an efficient way to test your employees' skills and measure their progress. A test provides data on which employees have been baited by the phishing email by clicking on the corresponding links. Your users can learn to identify suspicious emails and apply security awareness best practices by having the chance to experience a phishing attack.

Simulating phishing is an efficient way to test your employees' skills and measure their progress. A test provides data on which employees have been baited by the phishing email by clicking on the corresponding links. Your users can learn to identify suspicious emails and apply security awareness best practices by having the chance to experience a phishing attack.

CYBERS

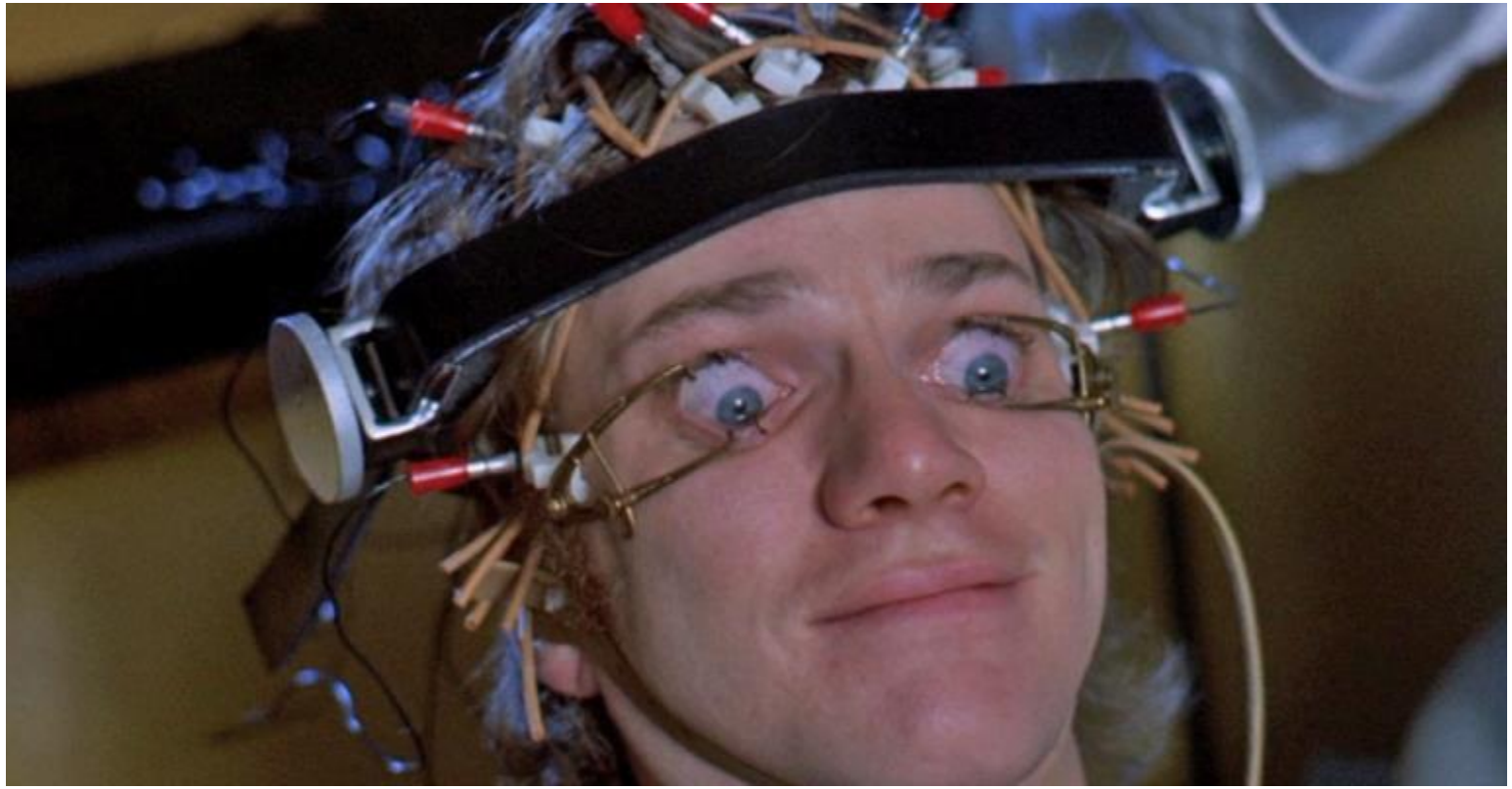


Most CISOs recognize the value of phish testing. By sending phishing emails generated by a company's IT department rather than a malicious attacker, **phishing simulation** provides insight into how well **phishing training** programs are working and which employees are most likely to be susceptible to a phishing email.

Most CISOs recognize the value of phish testing. By sending phishing emails generated by a company's IT department rather than a malicious attacker, **phishing simulation** provides insight into how well **phishing training** programs are working and which employees are most likely to be susceptible to a phishing email.

With employees being 40% more likely to encounter a phishing scam since 2021, now is a good time for decision-makers to assess and strengthen staff awareness by 'phishing their own pond' through internal attack simulations — but how exactly do these work?

With employees being 40% more likely to encounter a phishing scam since 2021, now is a good time for decision-makers to assess and strengthen staff awareness by 'phishing their own pond' through internal attack simulations — but how exactly do these work?



SNAKE OIL?

2023 DBIR

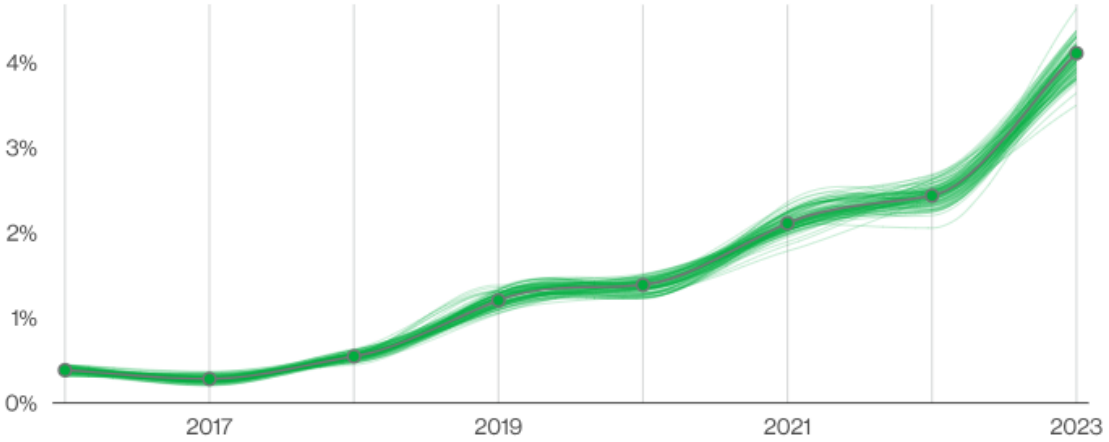


Figure 5. Pretexting incidents over time

Social Engineering attacks are often very effective and extremely lucrative for cybercriminals. Perhaps this is why Business Email Compromise (BEC) attacks (which are in essence pretexting attacks) have almost doubled across our entire incident dataset, as can be seen in Figure 5, and now represent more than 50% of incidents within the Social Engineering pattern.

https://www.verizon.com/business/resources/reports/dbir/2023/summary-of-findings/

2022 DBIR

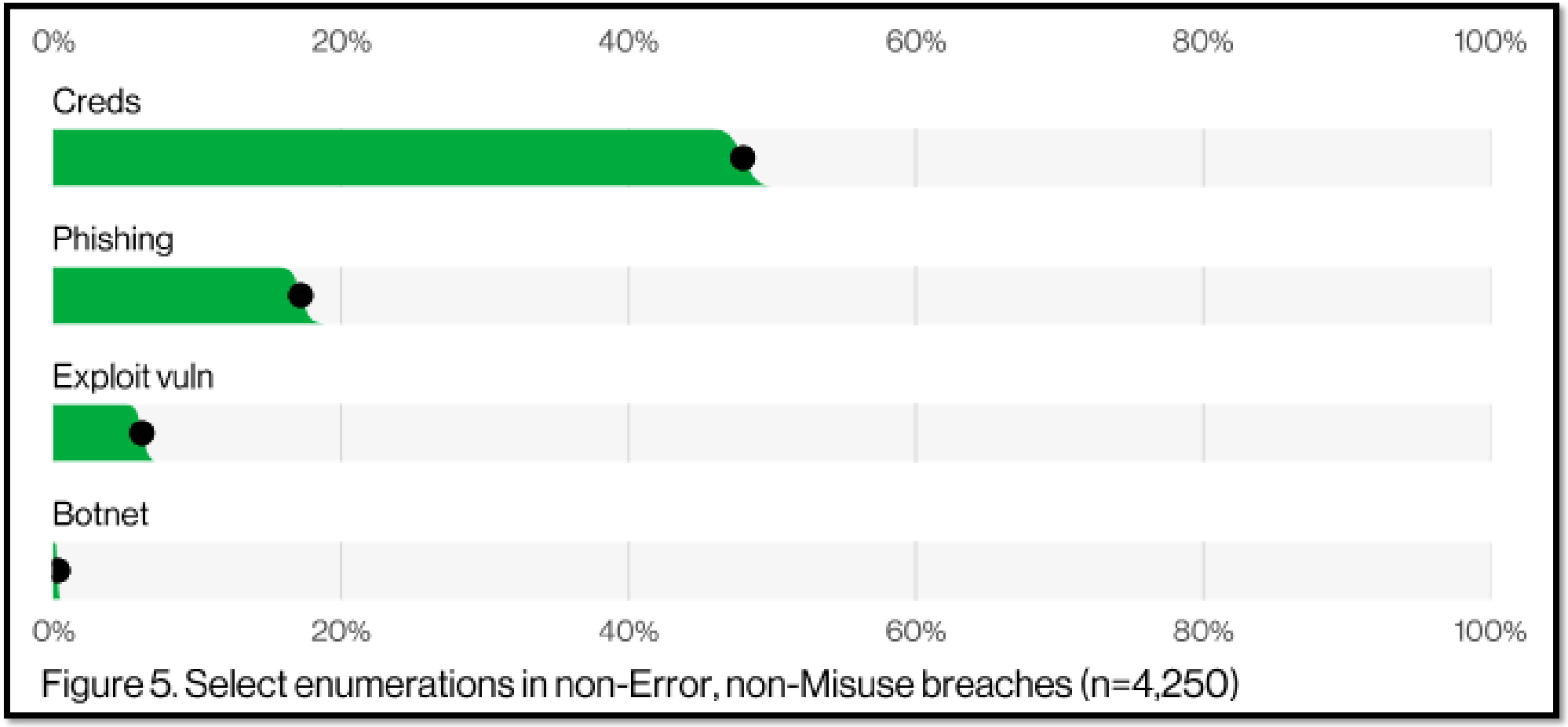


Figure 5. Select enumerations in non-Error, non-Misuse breaches (n=4,250)

https://www.verizon.com/business/resources/reports/dbir/2022/summary-of-findings/

2021 DBIR

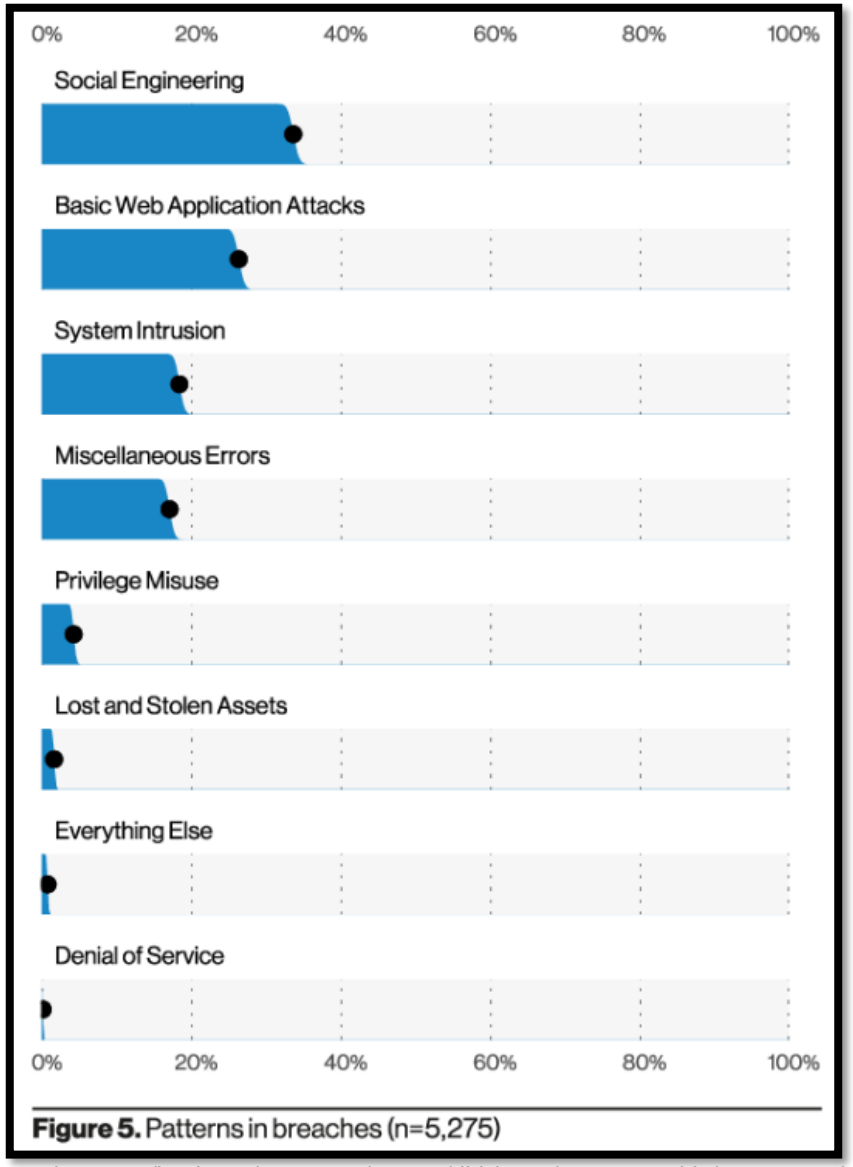
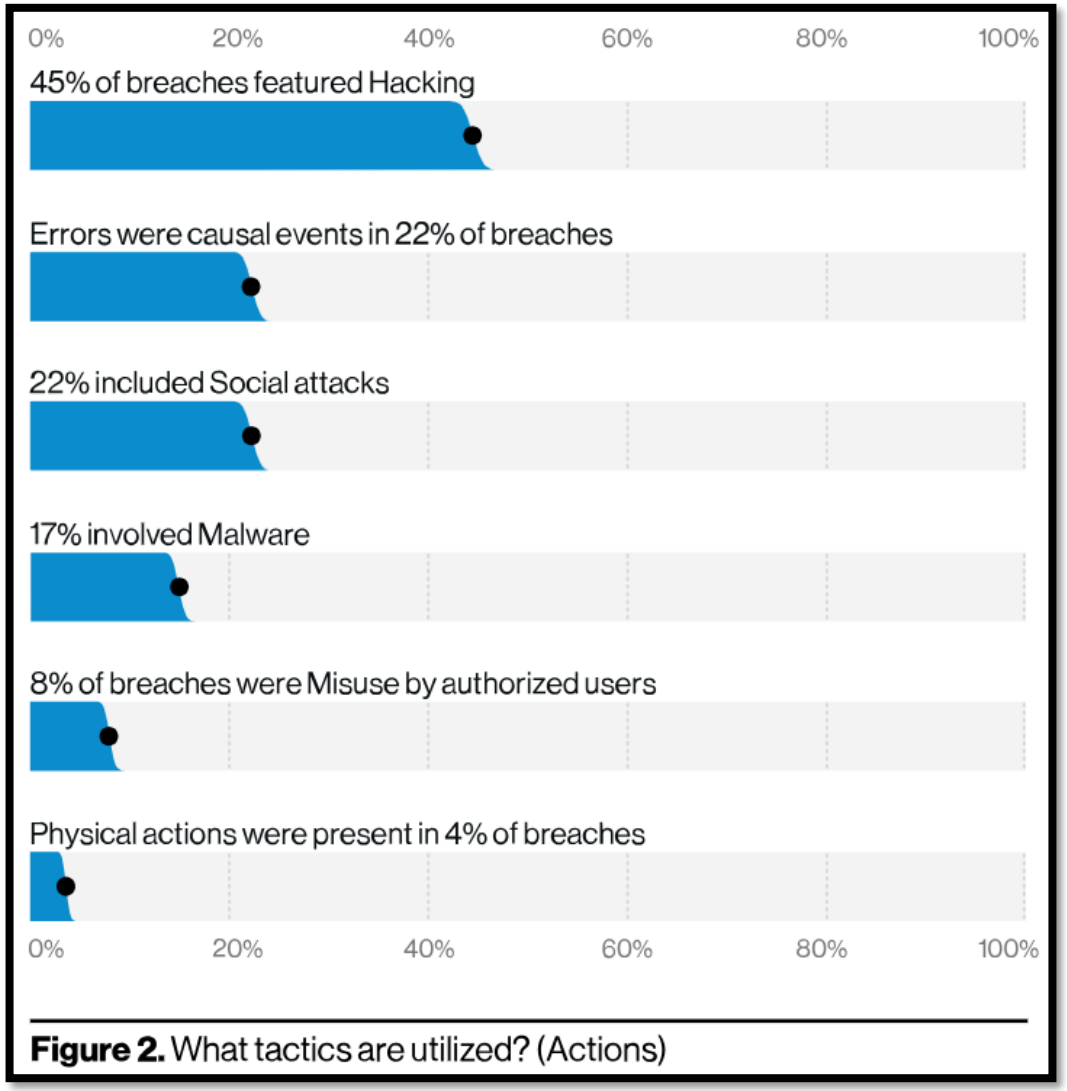


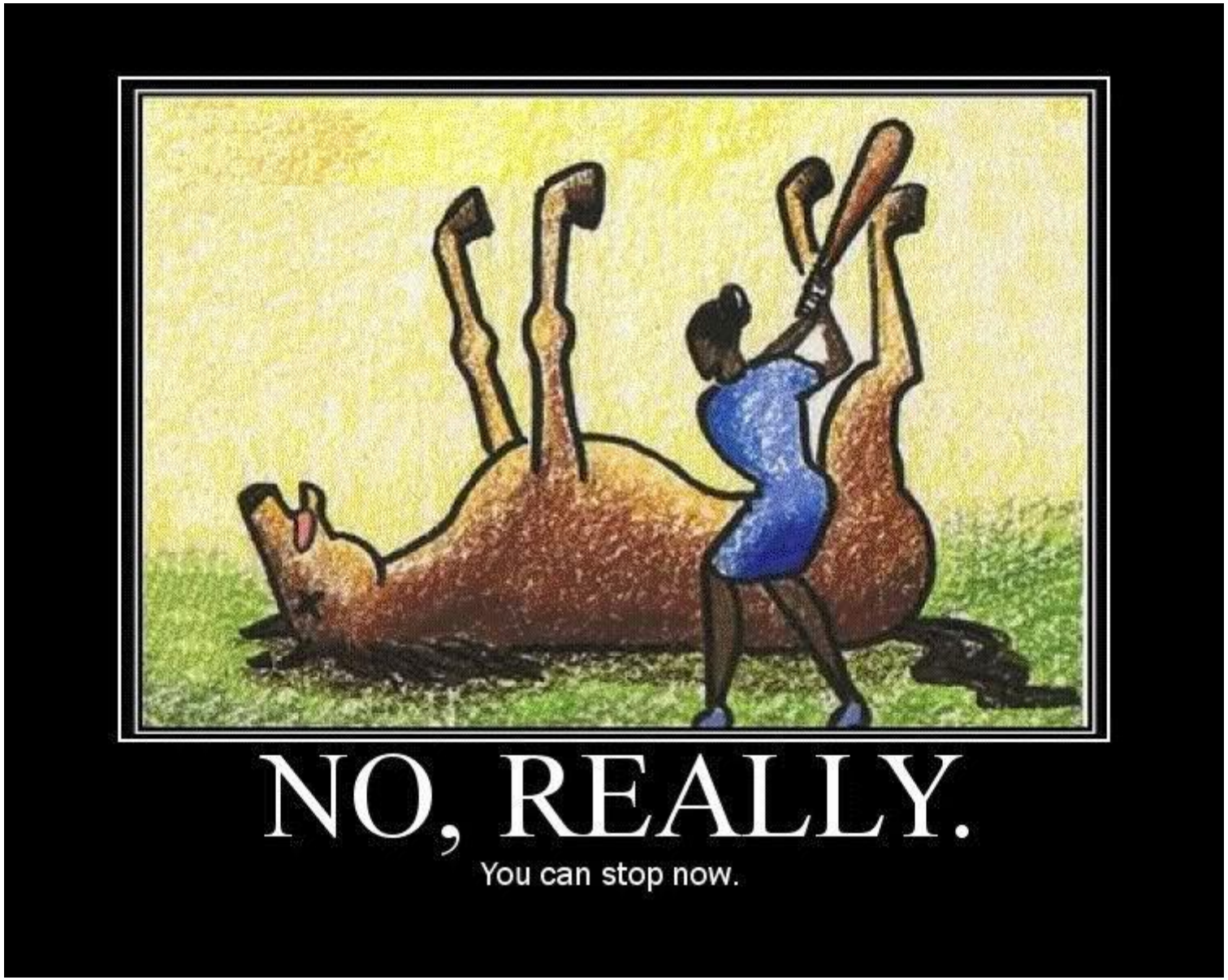
Figure 5. Patterns in breaches (n=5,275)

https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/summary-of-findings/

2020 DBIR



https://www.verizon.com/business/resources/reports/dbir/2020/summary-of-findings/



So….SNAKE OIL?

YES - IF

- Program is designed to make people aware of how to spot a phishing email
- Program focuses on vanity metrics
- Program lacks **context**

MOVING FORWARD

WHO CLICKED?

- "10% of users clicked the last phishing test email"
- Who cares?
  - Really.
- If the email gets to the right person at the right time they will click
- Vanity metrics totally miss the mark
  - If you get 0% clicks, the test is probably not realistic
  - If you put in the effort, you could approach 100% clicks

MEASURE WHAT MATTERS

- What is the time difference between the first “fail” and the first report?
  - Get the IR started!
- How many “fails” happed after the first report?
  - Even better to compare to your response time to real reports
- Assuming training focuses on reporting – how many recipients reported? Is this trending in the right direction?
- How many non-test true-positive phishes are being reported?

CHANGING BEHAVIORS

- Focus on realistic end-user actions – they're not all cyber experts
- We've tried the stick for years – let's try the carrot now
- You must continually check the tests against real world
  - Scenario
  - Tactics
  - RESULTS

CLOSING THOUGHTS

CLOSING THOUGHTS

- Stop focusing on WHO clicked
  - This is the new “our FW blocked 10,000,000 attacks last month”
- Identify the actions you want changed and build processes to reinforce them
  - Stop saying “don’t click” – you might as well say “stop using email”
- Measure results against REAL attacks
  - We all get bombarded with phishing emails

QUESTIONS

SEAN D. GOODWIN, GSE

Senior Manager, DenSecure

SDGoodwin@wolfandco.com

617.261.8139

https://www.linkedin.com/in/0xseang/

https://twitter.com/0xSeanG

https://www.wolfandco.com/services/densecure/

ABOUT WOLF & COMPANY, P.C.

111

YEARS IN BUSINESS

- Established in 1911
- Built on quality and integrity
- Succession strategy to remain independent allows us to be with you throughout your business lifecycle

300+

EXPERIENCED, HIGHLY TRAINED PROFESSIONALS

- Lower-than-industry-average staff turnover means a consistent team structure year after year
- Niche team dedicated to your industry

RESOURCES TO LEARN MORE

- Cultures & Values
- Inclusion & Diversity
- Our History
- Social Responsibility
- Thought Leadership
- Wolf Global

Wolf & Company ranked

#2 BEST LARGE FIRM TO WORK FOR

nationwide

accountingTODAY

WOLF & COMPANY, P.C.

den secure by wolf & company, p.c.

ABOUT WOLF & COMPANY, P.C.

SERVICES WE OFFER

We combine industry expertise with service specialization to provide your organization with insight, opportunities, and solutions allowing you to address your unique business needs.

ADVISORY

- Business Continuity Planning
- Cybersecurity
- Enterprise Risk Management
- Environment, Social & Governance
- Internal Audit
- IT Audit
- Model Risk Management
- Outsourced Accounting Solutions
- Penetration Testing
- Regulatory Compliance
- Strategic Planning

ASSURANCE

- Employee Benefit Plan Audits
- Financial Statements Audits
- HITRUST
- PCI DSS
- SOC Reporting

TAX

- Business Tax
- Federal
- International
- State & Local
- Private Client Group

vSUITE

- Virtual Consulting Services
  - Business Continuity Planning (BCP)
  - Virtual Chief Information Security Officer (vCISO)
  - Virtual Chief Privacy Officer (vCPO)
  - Virtual Chief Risk Officer (vCRO)
  - Virtual Vendor Management

WOLFPAC

- Integrated risk management SaaS suite

WOLF & COMPANY, P.C.

den secure by wolf & company, p.c.

WOLF ACCOLADES

Wolf is pleased to have received recognition from a variety of sources for our efforts at providing responsive client service and development of our professionals. Examples of this recognition include:

INSIDE Public Accounting

TOP 100
Accounting Firms

accountingTODAY

TOP 100
Accounting Firms

#2 BEST LARGE FIRM to Work For Nationwide

TOP FIRMS:
New England

BOSTON BUSINESS JOURNAL

- Area's Best Places to Work
- Area's Most Admired Companies
- Area's Fastest Growing Private Companies
- Area's Largest I.T. Consulting Firms

Forbes

America's Best
Tax and Accounting Firms of 2023, 2021

WOLF & COMPANY, P.C.

den secure by wolf & company, p.c.

ABOUT WOLF & COMPANY, P.C.

1911 **WOLF & CO. ESTABLISHED**

300+ **PROFESSIONALS**

3 OFFICES IN:

- Boston, MA
- Springfield, MA
- Livingston, NJ

SERVICES OFFERED IN:

- Audit
- Tax
- Risk Management

ABOUT DENSECURE

Wolf & Company's IT Assurance & Advisory team of cybersecurity experts, DenSecure™, brings together extensive technical knowledge and industry experience with internationally-recognized frameworks to develop strong cybersecurity programs.

DenSecure's core services include:

- Advanced Security Assessment
- Application Penetration Testing
- Network Penetration Testing
- Social Engineering
- Threat Emulation

Back to Home ⟶