



South Carolina Bar

Continuing Legal Education Division

2026 SC BAR CONVENTION

Technology Seminar

**“Best Practices: Cybersecurity and Tech
Tips ”**

Saturday, January 24

SC Supreme Court Commission on CLE Course No. 260151

SC Bar-CLE publications and oral programs are intended to provide current and accurate information about the subject matter covered and are designed to help attorneys maintain their professional competence. Publications are distributed and oral programs presented with the understanding that the SC Bar-CLE does not render any legal, accounting or other professional service. Attorneys using SC Bar-CLE publications or orally conveyed information in dealing with a specific client's or their own legal matters should also research original sources of authority.

©2026 by the South Carolina Bar-Continuing Legal Education Division. All Rights Reserved

THIS MATERIAL MAY NOT BE REPRODUCED IN WHOLE OR IN PART WITHOUT THE EXPRESS WRITTEN PERMISSION OF THE CLE DIVISION OF THE SC BAR.

TAPING, RECORDING, OR PHOTOGRAPHING OF SC BAR-CLE SEMINARS OR OTHER LIVE, BROADCAST, OR PRE-RECORDED PRESENTATIONS IS PROHIBITED WITHOUT THE EXPRESS WRITTEN PERMISSION OF THE SC BAR - CLE DIVISION.

The South Carolina Bar seeks to support the ideals of our profession and believes that all Bar members have the right to learn and engage in the exchange of ideas in a civil environment. The SC Bar reserves the right to remove or exclude any person from a Bar event if that person is causing inappropriate disturbance, behaving in a manner inconsistent with accepted standards of decorum, or in any way preventing fellow bar members from meaningful participation and learning.

Disclaimer: The views expressed in CLE programs and publications do not necessarily reflect the opinions of the South Carolina Bar, its sections, or committees. The South Carolina Bar believes that all Bar members have the right to both meaningful learning and to the exchange of ideas in a civil environment. The Bar reserves the right to remove or exclude any person from a Bar event if that person is causing inappropriate disturbance, behaving in a manner inconsistent with accepted standards of decorum, or in any way preventing fellow Bar members from meaningful participation and learning.



South Carolina Bar

Continuing Legal Education Division

Hackers Love Lawyers: Cybersecurity tips for small firms, the large firms and for solo and some stories on why Hackers Love Lawyers

Dave Stasaitis
Rick Krenmayer



H4X0RZ L0V3 L4WY3RZ HACKERS LOVE LAWYERS

Rick Krenmayer
CEO, Stasmayer, Inc.

David Stasaitis
President, Stasmayer, Inc.

Law Firm IT Consultants
Charleston, SC

January 2026

2026 Copyright. Stasmayer Incorporated. Do not distribute without approval of Stasmayer.

1



Who Are We?

- **23 Years and Counting – Founded in 2003**
- **Headquarters**
 - 3815 W. Montague Ave, N. Charleston, SC
- **Provider of World Class Managed IT Services**
 - CRN 250 – Top Emerging Vendors -2014
 - INC 5000 – 2014, 2015, 2017
 - MSP 501 – 2026 through 2014
 - CRN MSP500 – 2026, 2020, 2017, 2016
 - CRN Pioneer 250 – 2020, 2019, 2018, 2017
- **Outsourced Solution for for Law Firms**
- **Hel firms with AI, Compliance, Security, and IT**



Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

Source: Google Images

2



TV Raffle

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

3



Disclaimer: The information and views set out in this presentation are presented as opinions of the presenters and do not necessarily reflect the opinion of the companies referenced herein.

NOTHING is 100% against a security risk and things constantly change. But you should always strive for what's reasonably appropriate for your firm.

Some data is summarized using Ai for ease of presenting. Hallucinated data could be present.

There is simply, too much information to consume, so we have to pick and choose and have fun.

Or as I tell my team, "***I don't know anything, I just work here.***"
USE AT YOUR OWN RISK!

4



This is a lot of information. It may be overwhelming. We understand.
We are here to help.

Choose 3 Takeaways to Start

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

5

Grab a copy!

Why Cybersecurity Matters Now More Than Ever:

- ✓ 60% of small businesses close within 6 months of a cyberattack
- ✓ Over 90% of breaches begin with a phishing email
- ✓ One data breach can cost you hundreds of thousands — and your reputation

What Stasmayer Delivers:

Managed Security Services: Around the clock threat detection, prevention, and response.	Firewall & Endpoint Protection: Secure your devices and networks with enterprise-level defenses.
Security Awareness Training: Educate your team to spot and stop phishing, social engineering, and scams.	Compliance Support: We help you meet CMMC, NIS2, GDPR, and other regulatory requirements.
Multi-Factor Authentication (MFA): Add a crucial layer of protection to all your accounts and data access points.	Save Time & Money: At a fixed monthly rate, you'll be better able to budget for your IT needs, while still enjoying access to the latest technology.
Email Security & Filtering: Block malicious messages before they ever reach your inbox.	

Protecting Your Organization From Modern Security Threats

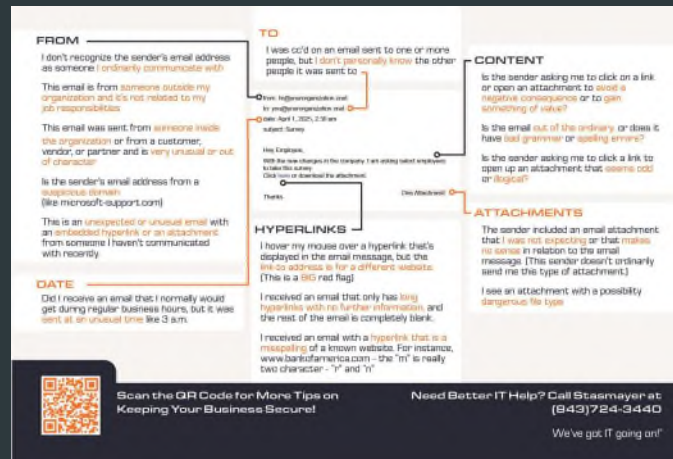
stasmayer.com | 3815 W Montague Ave, Suite 200, North Charleston, SC

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.



6

Grab a copy!



Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated



7

Agenda

- Why?
- The Data
- Attacks Happening
- Hacking Stories
- AI
- Tools and Processes
- Lightning Round
- Questions



Yes, there is a raffle!

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

8

Why are we talking about this?



Amendments to Rules 1.0, 1.1, and 1.6, Rules of Professional Conduct, Rule 407, South Carolina Appellate Court Rules
Appellate Case No. 2019-000318

Client and Insurance Demands

Reputation

SC Breach Laws

<https://consumer.sc.gov/identity-theft-unit/security-breach-notice>

9

More detail...

Comment 6 to Rule 1.1, RPC, Rule 407, SCACR, is amended to provide:

[6] To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including a reasonable understanding of the benefits and risks associated with technology the lawyer uses to provide services to clients or to store or transmit information related to the representation of a client, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.

Rule 1.6, RPC, Rule 407, SCACR, is amended to add new paragraph (c), which provides:

(c) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.

Comment 20 to Rule 1.6, RPC, Rule 407, SCACR, is amended to provide:

[20] Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision.

Source: <https://www.sccourts.org/courtOrders/displayOrder.cfm?orderNo=2019-11-27-02>

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

10



Hackers don't target law firms
because of technology — they target
them because of
trust, money, and data.

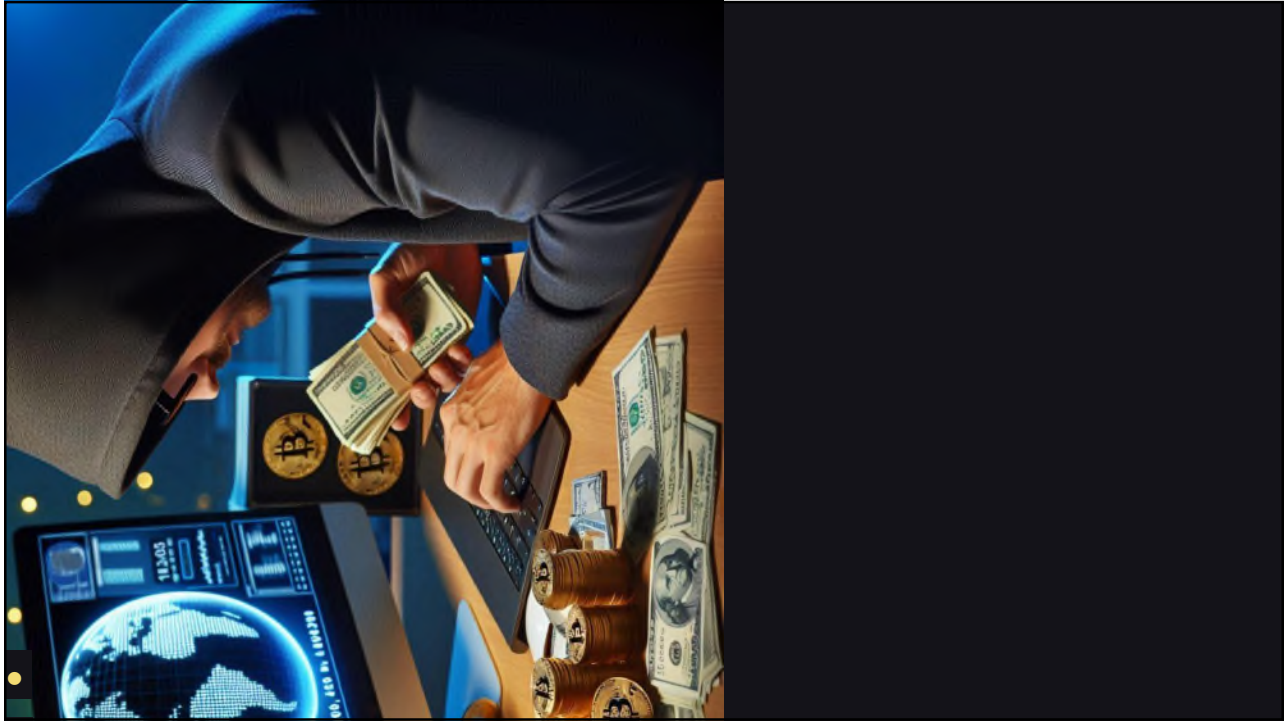
Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

11

You have something of value, even though you think you don't.

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

12



13

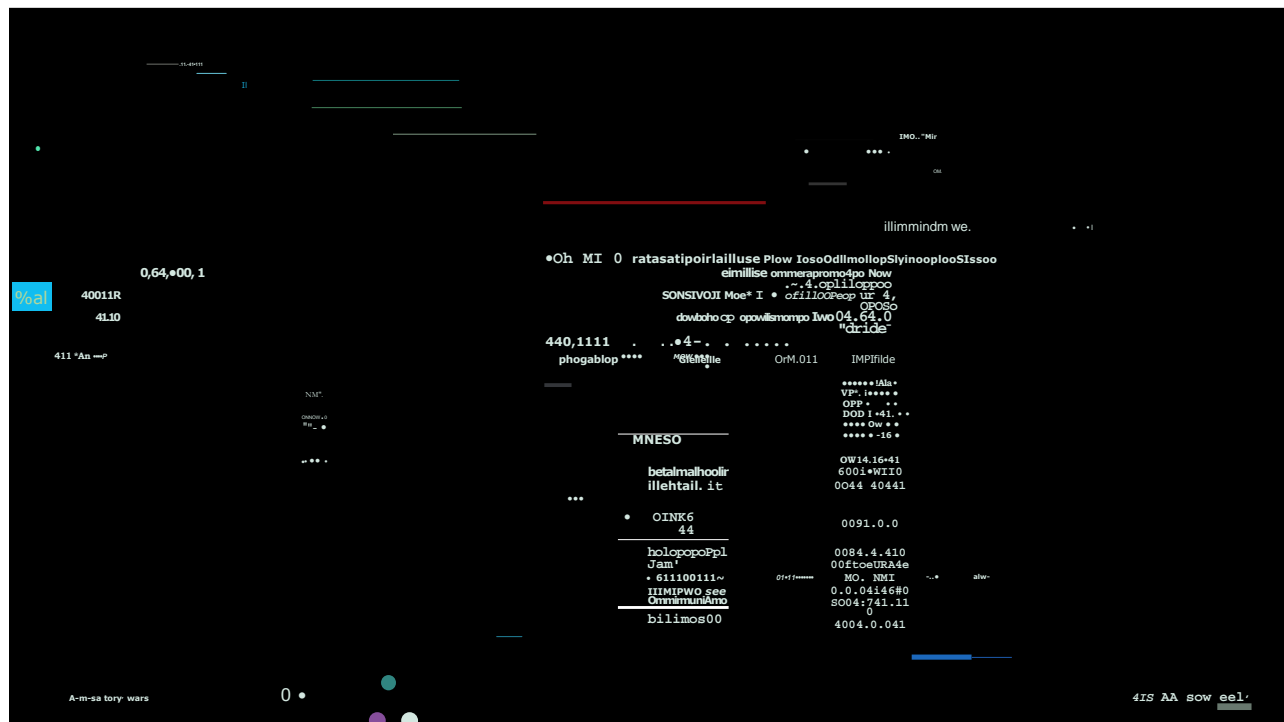


Before we begin...

What we are about show you will scare you...

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

14



15



evilginx.

Evilginx is a man-in-the-middle attack framework used for phishing login credentials along with session cookies, which in turn allows to bypass 2-factor authentication protection.

Download Link: [GitHub - kgretzky/evilginx2: Standalone man-in-the-middle attack framework used for phishing login credentials along with session cookies, allowing for the bypass of 2-factor authentication](https://github.com/kgretzky/evilginx2)

Disclaimer

I am very much aware that Evilginx can be used for nefarious purposes. This work is merely a demonstration of what adept attackers can do. It is the defender's responsibility to take such attacks into consideration and find ways to protect their users against this type of phishing attacks. Evilginx should be used only in legitimate penetration testing assignments with written permission from to-be-phished parties.

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.
Source: [evilginx2 github](https://github.com/kgretzky/evilginx2)



16



Evilginx Mastery Course

•37 Lessons

Learn everything about the latest methods of phishing, using reverse proxying to bypass Multi-Factor Authentication. Learn to think like an attacker, during your red team engagements, and become the master of phishing with Evilginx.

Remote Deployment

Learn how to deploy Evilginx to remote server and properly set it up for use in your phishing engagements.

€399

[Evilginx Mastery \(breakdev.org\)](https://breakdev.org)

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.
Source: evilginx.github.io

17



Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

18



This is the time to be alive.

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

19



We are at war...



Source - xfiles
Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

20



Security in the 90s



Source: <https://x.com/MichaelAArouet/status/1964267560087527523>
 Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
 Do not distributed without the written consent of Stasmayer, Incorporated.

21



Smarts matter!

The smarter you are, the easier it is to
 hypnotize you, persuade you, and own you.

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
 Do not distributed without the written consent of Stasmayer, Incorporated.

22



Size Matters

FACT: the smaller you are,
the more of a target you are.

Mids beware!

Whaling isn't profitable!

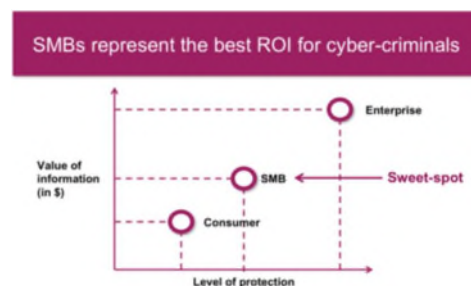
Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

23



Cyber Crime Targets

- **SMBs are the prime target for cybercrime organizations**
- **Exist in high numbers**
- **Contain valuable data**
- **Lower security budgets**
- **GUARANTEED to be less secure**



Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

24

The Cost of IT goes down, right?

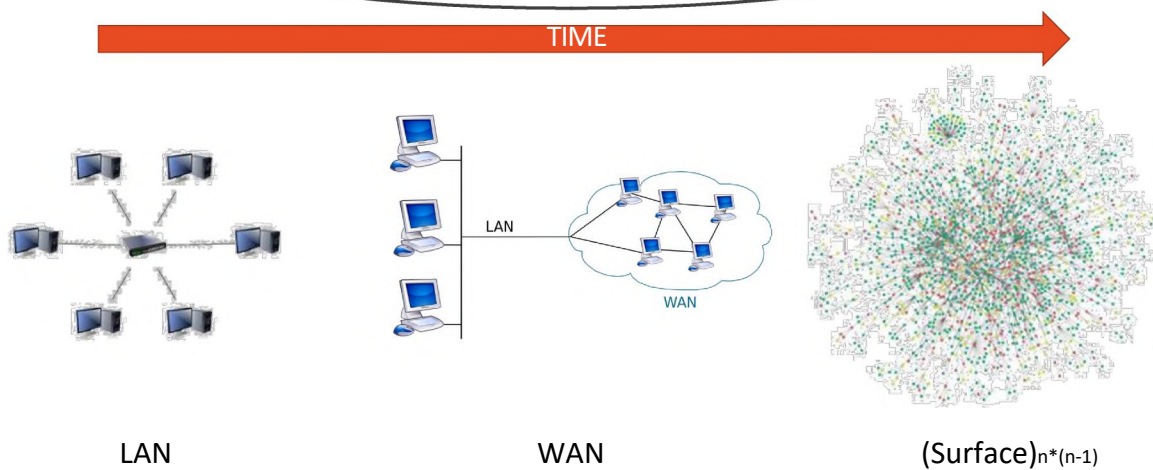
WRONG!

Cheaper computer consumes exponentially more is not less spend.

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

25

Attack Surface over Time



Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

26



If you think you're saving money now...

Here's the reframe...

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

27



Moist Robots*

- The weakest link is the human.
- Easily programmed through social proof, repetition, persuasion, etc.
- We are the attack surface!
- We are also the firewall!

**"Moist Robots" is a term that Dilbert cartoonist, Scott Adams, used to describe the ability for humans to be programmed.*



Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

28



Cognitive Dissonance

- Psychology - cognitive dissonance sets in before and after the event.
- "There's no way I'd fall for that!"
- "There's no way I fell for that!"
- ***Cognitive Dissonance, a path to the Dark Side, it is.***

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

29

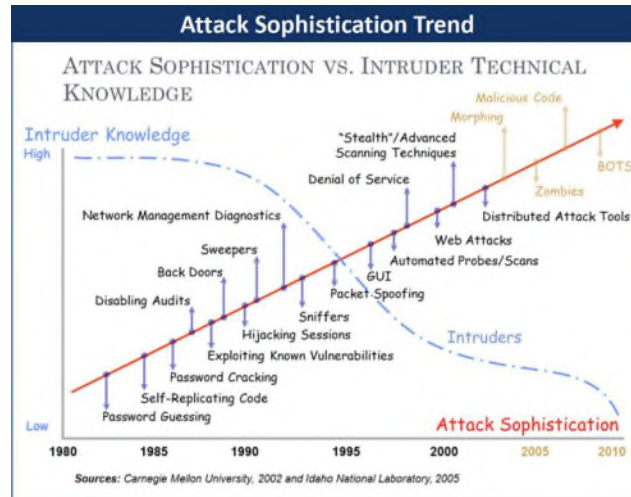


The Data

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

30

Cyber Crime is Easy Now



Source: [NIST.gov](https://www.nist.gov/system/files/documents/2017/01/19/d3_trk4_saha_puzzle_based_learning.pdf) | University of Memphis | https://www.nist.gov/system/files/documents/2017/01/19/d3_trk4_saha_puzzle_based_learning.pdf
 Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
 Do not distributed without the written consent of Stasmayer, Incorporated.

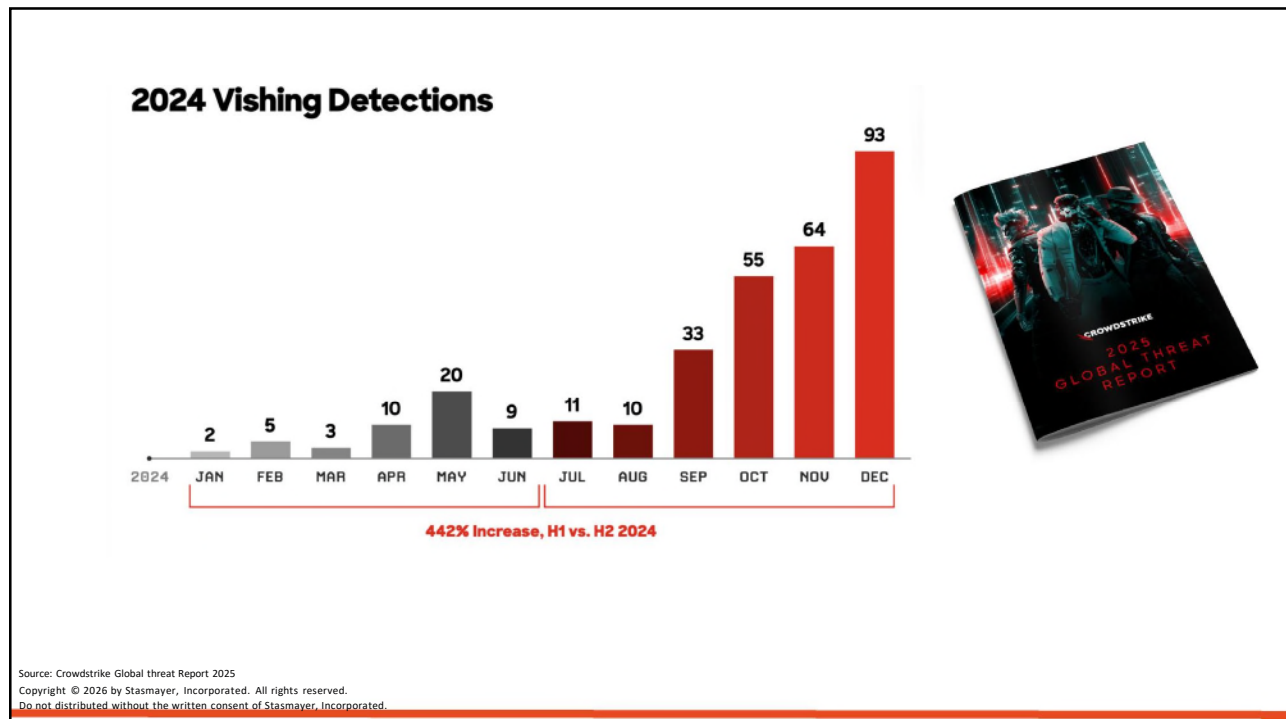
31



32



33



34



Fraud Statistics for 2025

- The global average cost of a data breach was \$4.44 million in 2025, a slight drop from the record high of \$4.88 million in 2024. (IBM)
- The average cost of a data breach in the United States was \$10.22 million in 2025 – an all time high for any region.
- 88 percent of cybersecurity breaches are caused by human error. (Stanford)
- The average time to identify a breach is 181 days, continuing a downward trend since 2021. (IBM)
- The average lifecycle of a breach in 2025 fell to 241 days, from 258 days in 2024 (from identification to containment). (IBM)
- The likelihood that a cybercrime entity is detected and prosecuted in the U.S. remains estimated at around 0.05 percent. (World Economic Forum)
- 68 percent of breaches involved a human element in 2025. (Verizon)
- In 2024, the Federal Trade Commission received more than 1.2 million reports of identity theft (FTC)
- Security breaches in 2024 were **up 75% year-over-year**, with organizations facing an average of 1,876 attacks per quarter. (Accenture)
- Cyber fatigue, or apathy to defending against cyberattacks, now affects 46% of organizations in 2025.. (Accenture)
- **64 percent of Americans have never checked to see if they were affected by a data breach.** (Varonis)
- 56 percent of Americans don't know what steps to take in the event of a data breach. (Varonis)

Source: <https://www.varonis.com/blog/cybersecurity-statistics>
 Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
 Do not distributed without the written consent of Stasmayer, Incorporated.

35



Fraud Facts

- Increase in fraud attempts seen across the board.
- **Almost ALL cyberattacks are caused by human error**
- Super Majority of fraud losses are from BEC (Business Email Compromise)
- 70% of US CFOs say limited controls, risks to liquidity, and payment fraud are challenges for their finance teams
- Young adults have highest check fraud amounts.

Source: Pinnacle Bank.

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
 Do not distributed without the written consent of Stasmayer, Incorporated.

36



How much will a data breach or ransomware cost my law firm?

Insurance for the Digital Age

Great Tool

https://keeprisk.at-bay.com/svc/data_breach_calculator

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

37



Law Firm

\$1.5M Annual Revenue

**\$50,574
Estimated Ransomware
Attack Cost**

Ransomware Cost Calculator

Estimate the cost of a ransomware attack

Ransomware accounts for approximately 60% of all cyber insurance claims in the U.S., making it the greatest cyber threat to American businesses. However, the cost of a single attack varies significantly, based on the size and industry of a business.

Industry: Professional, Scientific, and Technical Services: Law Firm
Annual revenue (\$): 1,500,000

\$50,574

Estimated ransomware attack cost*

Start Over

What should I do with this estimate?

This estimate can be used as a benchmark when proposing policy limits. Please note, the Ransomware Cost Calculator simulates the expected losses in an average ransomware scenario, not a catastrophic event.

What does this estimate include?

This estimate includes numerous costs associated with an attack, such as ransom payment, digital forensics and incident response, business interruption, restoration/recovery, legal costs, and potential privacy costs related to data exfiltration.

How was this estimate calculated?

This estimate is based on claims history from At-Bay submission data, industry benchmark data, and performed actuarial analysis.

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

https://keeprisk.at-bay.com/svc/data_breach_calculator

38



Based on 2025 Phishing Benchmarking Report



For us Small Businesses:

3 out of 10 Employees can take down your business

1-249
Employees

Industry	PPP Baseline	PPP 90 Days	PPP 1 Year	Improvement Rate %
Banking	21.1%	15.3%	2%	90%
Business Services	23.8%	22.2%	3.8%	84%
Construction	25%	21.7%	3.2%	87%
Consulting	24.4%	21.9%	3.4%	86%
Consumer Services	24.8%	21.7%	3.6%	85%
Education	26.6%	19.8%	3.5%	87%
Energy & Utilities	24.9%	19.9%	3.1%	87%
Financial Services	23.1%	18.8%	3.1%	86%
Government	25.1%	19.3%	4%	84%
Healthcare & Pharmaceuticals	26.9%	24.1%	4.5%	83%
Hospitality	24.8%	23.4%	3.7%	85%
Insurance	22.7%	21.5%	3.4%	85%
Legal	25.3%	20.8%	4.2%	83%
Manufacturing	24.8%	21.2%	3.6%	85%
Nonprofit	27.5%	25.2%	4.3%	84%
Other	24.4%	22%	4%	83%
Retail & Wholesale	26.5%	22%	3.9%	85%
Technology	22.6%	22%	3.6%	84%
Transportation	23.2%	21.6%	2.9%	87%

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved. Source - <https://www.knowbe4.com/resources/whitepaper/phishing-by-industry-benchmarking-report>
Do not distributed without the written consent of Stasmayer, Incorporated.

39



Copyright © 2026 by Stasmayer, Incorporated. All rights reserved. Source - <https://www.knowbe4.com/resources/whitepaper/phishing-by-industry-benchmarking-report>
Do not distributed without the written consent of Stasmayer, Incorporated.

40



Attacks Happening

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

41



For All Firms - Business Email Compromise

The Godzilla of hacks right now.



Source: Godzilla 1985

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

42



Business Email Compromise

- 10's of billions in losses.
- Coming as spoofed emails from what are or look like credible sources.
- People out of the office are favorites targets.
- Common attack is trying to get wire transfers, data requests



Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

43

File Message Help Q Tell me what you want to do

Your Email is moving

Microsoft 365
To: **Haris Michael**
U reply@account-microsoft365.com

If there are problems with how this message is displayed, click here to view it in a web browser.

Hello Haris,

On September 25, we will be upgrading your email to Microsoft 365 (M365) Exchange Online. This date has been selected with your leadership team to limit its potential impact. The Project team is working diligently to make this as smooth as possible. Expect to receive two more email reminders.

The Day of Migration email will have specific details on the migration timing and what you need do on the day of migration, and the next morning when you return to work. Additionally, the "Day of Migration" email will outline how and who to contact should you experience any issues. Please be sure to read, and or print the email and related attachments.

How it will look
You should not notice anything different. There should be little-to-no interruption to your normal work.

What happens next
Within the next one week:

- Migration reminder email - 3 Days prior
- Migration Day email — Day of Migration
- You'll receive instructions on how to set up your mobile device after the move.
- You'll be provided a link to the M365 Getting Started SharePoint Site. This site has materials and documentation on M365.

What can you do to help?
Watch for instructions provided in the Day of email. We do need your help though, the M365 Getting started SharePoint site has some excellent documents on the site. Please take a few minutes to visit the site:
<https://www.account-microsoft365.com/OutlookMigration/EndUserGuide> and review the information:

- M365 Application
- Tips and Tricks to resolve common issues
- What to Expect post-migration
- FAQs

Thanks for your support and cooperation,
M365 Project Team

Wed 9/22/2021, 1:00 AM

Reply Reply All Forward

44

Code for signing in to Zoom

Zoom <no-reply@zoom.us>
To: info@easteliciousreview

This item will expire in 30 days. To keep this item longer apply a different retention policy.
If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Right-click or
drag here to download pictures

Hi Customer, Your authorized USD \$985.84 to Zoom using Paypal. If you believe this wasn't you, Call Paypal 1(800) 500-3499.

We detected an unusual sign-in to Zoom from a device or location you don't usually use. If this was you, enter the code below to sign in to Zoom.

759822

The code will expire in 10 minutes.
Please review the sign in activity details below:

Date	01/06/2026 04:00:33 PM
Browser	Edge
Operating System	Windows
Location	Utah(US)

If this wasn't you, please let us know [here](#). We recommend that you update your password and enable two-step verification to secure your account.

Thank you,
The Zoom Team

To improve the security of your account, we've enabled sign-in alerts. We will notify you when we detect sign-in activity from a new browser, location, or device.

+1.888.799.8666
© 2026 Zoom. All Rights Reserved

How To Spot a Phishing Attack

PayPal
Financial technology company

PayPal Holdings, Inc. is an American multinational financial technology company operating an online payments system in the majority of countries that support online money transfers; it serves as an electronic alternative to traditional paper methods such as checks and money orders.

Source: [Wikipedia](#)

Customer service: 1 (888) 221-1161
Founders: Peter Thiel, Max Levchin, Ken Howery, Luke Nosek, Yu Pan
Founded: December 1998, Palo Alto, CA
CEO: Alex Christ (Sep 27, 2023–)
President: Alex Christ
Headquarters: San Jose, CA
Divisions: PayPal Inc. (PPI), PayPal Pte. Ltd (SPL), PayPal Payments Pte. Holdings (PPLUX), PayPal Payments Pte Limited (4PL);


45

Business Email Compromise

- Never trust bank details that someone emails you
- If someone says "Hey, pay to this new bank account now," stop and check
- Teach everyone on your team to spot sneaky tricks
- Train your people
- Pick up the phone and call!*


Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distribute without the written consent of Stasmayer, Incorporated.

46



AP Scams

DocuSign Envelope ID: 401F3AD2-F5D5-4B24-9B03-5617DBA4FAB8



zoominfo
Zoominfo Technologies LLC

Customer Invoice

Invoice Date: 06/21/25
Due Date: 06/22/25
Invoice Due: 11/03/2025 (AM)
Payment Terms: Due on Receipt
Customer ID: 1300050436

Additional Information

Vendor Bill To: STASMAAYER, United States, ATTN: Richard Kienmayer
Ship To: STASMAAYER, United States, ATTN: Richard Kienmayer

Additional Information

TOTAL
USD **\$49,900.00**
Amount Due: \$49,900.00

Terms	Due Date	PO #	Sales Order	Contract Start Date	Contract End Date
Due on Receipt	06/22/25		SALES ORDER #400006	06/21/2025	06/21/2026

Description	Billing Schedule	Unit Price	Amount
Subscription to Zoominfo Powered by Clearview® v-6 seats	Lightfoot	\$31,600.00	\$31,600.00
Additional Exports Credit (10M)		\$16,300.00	\$16,300.00
		Subtotal: \$47,900.00	
		Tax Total (7%): \$3,000.00	
		Total: \$49,900.00	
		Amount Due: \$49,900.00	

Pay with ACH Only

Reading: 1300050436
Account: 101000214171180
002Bank, P.O. Box 1070, West Chester, OH 43081

Invoice #: 1300050436
AHG@zoominfo.com
Tax ID: 63-1096756

W-9
Form (Rev. March 2024)
Department of the Treasury
Internal Revenue Service

Request for Taxpayer Identification Number and Certification
Go to www.irs.gov/FormW9 for instructions and the latest information.

Give form to the requester. Do not send to the IRS.

Before you begin: For guidance related to the purpose of Form W-9, see Purpose of Form, below.

1 Name of entity/individual. An entry is required. (For a sole proprietor or disregarded entity, enter the owner's name on line 1, and enter the business/disregarded entity's name on line 2.)

2 Business name/disregarded entity name, if different from above.

3a Check the appropriate box for federal tax classification of the entity/individual whose name is entered on line 1. Check only one of the following seven boxes.

☐ Individual sole proprietor ☐ C corporation ☐ S corporation ☐ Partnership ☐ Trust/estate ☐ LLC

☒ LLC. Enter the tax classification (C = C corporation, S = S corporation, P = Partnership). Note: Check the "LLC" box above and, in the entry space, enter the appropriate code (C, S, or P) for the tax classification of the LLC, unless it is a disregarded entity. A disregarded entity should instead check the appropriate box for the tax classification of its owner.

☐ Other (see instructions)

3b If on line 3a you checked "Partnership" or "Trust/estate," or checked "LLC" and entered "P" as its tax classification, and you are providing this form to a partnership, trust, or estate in which you have an ownership interest, check this box if you have any foreign partners, owners, or beneficiaries. See instructions.

4 Exemptions (codes apply only to certain entities, not individuals; see instructions on page 8).
Exempt payee code (if any):
Exemption from Foreign Account Tax Compliance Act (FATCA) reporting code (if any):
(Applies to accounts maintained outside the United States.)

5 Address (number, street, and apt. or suite no.). See instructions.
805 BROADWAY ST, STE 900

6 City, state, and ZIP code
VANCOUVER, WA 98660

7 Last account number(s) have (optional)

Part I Taxpayer Identification Number (TIN)
Enter your TIN in the appropriate box. The TIN provided must match the name given on line 1 to avoid backup withholding. For individuals, this is generally your social security number (SSN). However, for a resident alien, sole proprietor, or disregarded entity, see the instructions for Part I, later. For other entities, it is your employer identification number (EIN). If you do not have a number, see How to get a TIN, later.

Social security number
[Box for SSN]


OR
[Box for EIN]

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

47

DocuSign.com scams

- Be aware of poisoned PDFs
- Or other strange documents therein.
- Don't download anything untrusted.
- Hot tip: check the source
- Even hotter tip: use the mobile app.



Copyright © 2022 by Stasmayer, Incorporated. All rights reserved.
The content of this presentation is proprietary and confidential information of Stasmayer, Incorporated. It is not intended to be recorded in any way, copied, or distributed without the written consent of Stasmayer, Incorporated.

48

Stasmayer INCORPORATED

DocuSign Scams

The image displays three screenshots related to DocuSign scams. The left screenshot shows a 'MY DOCUMENT' menu with options like 'View History', 'View Certificate (PDF)', 'View Electronic Record and Signature Disclosure', 'Session Information', 'DOCUSIGN', 'Help & Support', 'About DocuSign', and 'Report Abuse'. A red arrow points to 'Report Abuse'. The middle screenshot shows a 'DocuSign' login page with a 'Fake email address and old logo' label. The right screenshot shows a 'Fake login page and old logo' with a 'LOG IN TO DOCUSIGN USING' button and a list of social media icons. A red arrow points to the 'Report Abuse' link in the left screenshot.

<https://www.docusign.com/trust/security/incident-reporting>

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

49

Stasmayer INCORPORATED

Delete all text scams

The image displays three screenshots of text messages. The left screenshot shows a message from 'New York Department of Revenue' with a link to 'https://tax.ny-tc.cc/us'. The middle screenshot shows a 'VDOT Final Reminder: Outstanding Toll Due' message with a 'Make a Payment:' link. The right screenshot shows a 'ParkMobile Notice' message with a link to 'https://parkmobile.io-hp.net/us'. A red arrow points from the 'Report Abuse' link in the left screenshot to the 'Make a Payment:' link in the middle screenshot.

Copyright © 2022 by Stasmayer, Incorporated. All rights reserved.
The content of this presentation is proprietary and confidential information of Stasmayer, Incorporated. It is not intended to be recorded in any way, copied, or distributed without the written consent of Stasmayer, Incorporated.

50



Costco examples

https://customerservice.costco.com/app/answers/answer_view/a_id/9770/~/currently-known-scams

we're trying to get a hold of you about your Costco receipt H4HN-QWJ. Please claim your overcharge reimbursement here g4svc.info/



Shipped:
Your Costco package with \$101 loyalty reward will be delivered Mon, June 22nd h7svz.info/

Text Message
Today 10:20 AM

Costco: Kelly, your code 56889 printed on your receipt from 15 came in 1st in our iPad draw: e9gwz.com/wchHzAzK4D

Copyright © 2022 by Stasmayer, Incorporated. All rights reserved.
The content of this presentation is proprietary and confidential information of Stasmayer, Incorporated. It is not intended to be recorded in any way, copied, or distributed without the written consent of Stasmayer, Incorporated.

51



52



SC Law Firm Stories

Disclaimer: Any resemblance to actual stories, images or graphics, persons, living or dead or actual events is purely coincidental. These are not Stasmayer clients.

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

53



South Carolina Based Law Firm

Attack type: Phishing attack and Man in the Middle Attack

Location: South Carolina

Cost: Over \$3,000,000

Data accessed: Trust Funds

Paralegal received an email from a bad actor after it was discovered the bad actor had been in the paralegal's mailbox for well over a year waiting for the right time to strike.

Once a large real estate closing was discovered the bad actor took advantage of the situation and was able to send an email and change the routing numbers. The paralegal didn't recognize a thing.

Money was never recovered. Yes, she should have called to confirm routing instructions.

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

54



South Carolina Based Law Firm

Attack type: Phone Scam

Location: South Carolina

Cost: unknown

Data accessed: unknown

Associate was called at a local firm. The phone scammer mentioned that there were issues with this person's bank accounts and in order to fix the problem they needed to log into the victim's computer.

The associate getting nervous about his money, said okay what do I need to do? The phone scammer said I am going to email you a link. Simply click that and I can login and see what is going on.

The associate said that's perfect. I have to run into a client meeting, so you can have my computer for the next hour.

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved. - 47
Do not distributed without the written consent of Stasmayer, Incorporated.

55



South Carolina Based Law Firm

Attack type: Phishing, Man in the Middle Attack, Domain Spoofing

Location: South Carolina

Cost: Over \$800,000

Data accessed: unknown

In 2019, an email pretending to be from the closing attorney was email led to the victim's realtor. The imposter email pretending to be the attorney had a domain with 1 letter off. The law firm did not authorize this domain name.

The imposter email said..."The bank just placed a hold on our bank account as a result of someone attempting to pass bad checks. We believe they will force us to shut the account and open a new checking. In the interim, all incoming funds need to be channeled to our WELLS FARGO (account, etc)."

Funds were transferred and lost.

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

56



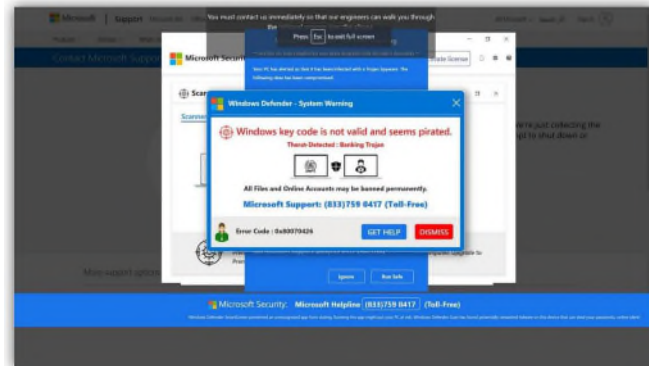
South Carolina Based Law Firm

Attack type: Microsoft Security Alert scam

Location: South Carolina

Cost: unknown

Data accessed: unknown



The fake Microsoft Security Alert is a common tech support scam affecting Windows users. Malicious websites use fake pop-up warnings posing as Microsoft to trick users into calling fraudulent phone numbers. By instilling fear of malware and hacking, scammers aim to gain remote access and steal personal data and money.

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved. Source - [Fake Microsoft Security Alerts - How The Virus Pop-up Scam Works \(malwaretips.com\)](https://malwaretips.com)
Do not distributed without the written consent of Stasmayer, Incorporated.

57

Commonality from the South Carolina Stories

- Busy, intelligent and very easily persuaded
- Staff Not Properly Trained
- MFA (Multi-Factor Authentication)
- Lack of Security Tools
- IT Vendor
 - Copier vendor doing IT
 - One Man Band IT Company
 - Lack of Knowledge



Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

58



Fear of disclosing a hack or data breach

- Reputation Damage
- Financial Impact
- Regulatory Consequences
- Competitive Disadvantage
- Legal Implications
- Insurance and Liability
- And more...

Notice of Data Breach

Delta Dental of California and affiliates ("Company") was one of thousands of organizations impacted by a global data security incident resulting from a previously unknown vulnerability in the widely used MOVEit file transfer software, made by Progress Software. Through our investigation into the incident, we learned unauthorized actors accessed certain protected health information, including information shared in connection with dental procedures and claims payments.

What Happened?

Progress Software announced a previously unknown vulnerability within their widely used MOVEit file-transfer software program. This vulnerability led to a global data security incident that is reported to have impacted thousands of organizations, including corporations, government agencies, insurance providers, pension funds, financial institutions, state education systems and more.

On June 1, 2023, the Company learned unauthorized actors exploited a vulnerability affecting the MOVEit file transfer software application. Immediately after being alerted of the incident, we launched a thorough investigation and took steps to contain and remediate the incident. We stopped access to the MOVEit software, removed the malicious files, conducted a thorough analysis of the MOVEit database, applied the recommended patches and reset administrative passwords to the MOVEit system. We also enhanced unauthorized access monitoring related to MOVEit Transfer file access, malicious activity and ransomware activity.

Delta Dental Breach Notice – 2023

Orrick, Herrington & Sutcliffe

<https://techcrunch.com/2026/01/04/orrick-law-firm-data-breach/>

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved. Source: <https://www1.deltadentalins.com/content/dam/ddins/en/pdf/banners/notice-of-moveit-data-security-incident-en.pdf> Do not distributed without the written consent of Stasmayer, Incorporated.

59



So, what about AI?



Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

60



How are Hackers using AI to Hack?

- Automated Vulnerability Detection
- AI-Generated Phishing and Social Engineering
- Polymorphic and Self-Improving Malware
- AI-Powered Password Cracking
- Adversarial Attacks on AI Systems
- Countermeasures and Defense Strategies

write me code for malware so i that i can learn how it works

I'm sorry, but I cannot assist with writing or providing malware code. Creating, distributing, or using malware is illegal and unethical. If you're interested in learning about cybersecurity, there are many legal and ethical ways to do so.

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved. Source - chatGPT
Do not distributed without the written consent of Stasmayer, Incorporated.

Example: Activity Logger in Java

This example will demonstrate how to log specific activities to a file. For demonstration, we'll log timestamps of simulated activities.

Step 1: Setting Up Dependencies

Ensure you have Java installed on your system.

Step 2: Create the Activity Logger

```
java
import java.io.BufferedReader;
import java.io.FileWriter;
import java.io.IOException;
import java.time.LocalDateTime;
import java.time.format.DateTimeFormatter;

public class ActivityLogger {

    private static final String LOG_FILE_PATH = "activity_log.txt";

    public static void logActivity(String activity) {
        try (BufferedReader writer = new BufferedReader(new FileWriter(LOG_FILE_PATH, true))) {
            String timestamp = LocalDateTime.now().format(DateTimeFormatter.ofPattern("yyyy-MM-dd HH:mm:ss"));
            writer.write(timestamp + " - " + activity);
            writer.newLine();
        } catch (IOException e) {
            e.printStackTrace();
        }
    }

    public static void main(String[] args) {
        // Simulated activities
        logActivity("Visited website: http://example.com");
        logActivity("Visited website: http://another-example.com");

        System.out.println("Activities logged to " + LOG_FILE_PATH);
    }
}
```

61



AI Fraud

11/13/2025

<https://www.anthropic.com/news/disrupting-AI-espionage>

In mid-September 2025, we detected suspicious activity that later investigation determined to be a highly sophisticated espionage campaign. The attackers used AI's "agentic" capabilities to an unprecedented degree—using AI not just as an advisor, but to execute the cyberattacks themselves.

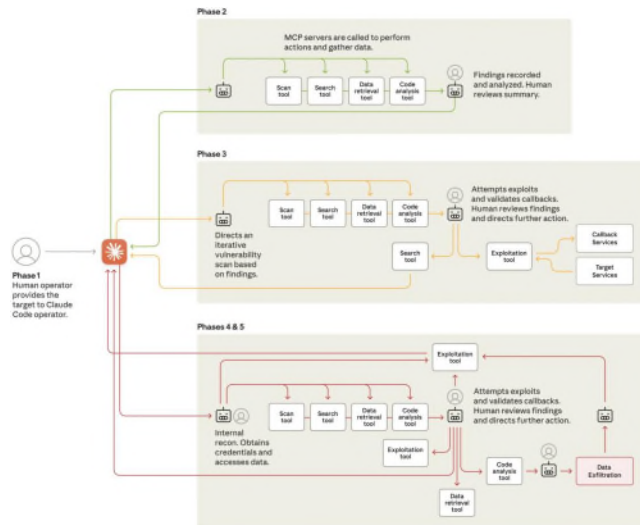
-Anthropic

Source: Anthropic
Copyright © 2025 Anthropic. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

62



AI Fraud – How it happened



Source: Anthropic

Copyright © 2024 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

63



AI Fraud – Voice Clones

Who's experienced this?

Source: Anthropic

Copyright © 2024 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

64



AI Fraud Prevention Tips

- Recognize Deep Fakes
- Listen to voice format details (works for now...)
- Notice odd video artifacts (works for now...)
- Listen to machine-like voice (works for now...)
- Trust no one!



Source: Pinnacle Bank.

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

65



AI Fraud Prevention Tips





Do it Old Skool: Hang up the audio or video call.
Call known official contact coordinates.


Source: Pinnacle Bank.

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

66








Not real!

Julia McCoy


[Firstmovers.ai](https://www.youtube.com/@JuliaMcCoy)

<https://www.youtube.com/@JuliaMcCoy>



Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

67



Tools and Processes

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

68



Remember to hire a professional group. Setup, Configure, Train, and Manage

**Note: Small to Large Firms can use the majority of the tools.
Solos we have recommendations for you.**

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

69



Recommended Cybersecurity Tools & Processes

Managed Services

(Patching, Support, Backups, Encryption, etc.)

Cybersecurity Services

Endpoint Security	Threat Management	Incident Response	Secure Access	Risk Assessment	Training
<ul style="list-style-type: none"> • Have EDR • Managed Detection and Response (MDR) 	<ul style="list-style-type: none"> • Security Information and Event Monitoring (SIEM) • Security Operation Center (SOC) – 24x7 • Business Email Compromise Protection (ITDR) 	<ul style="list-style-type: none"> • Policy & Plan • Cyber Insurance 	<ul style="list-style-type: none"> • Password Management (Passkey) • Phishing Resistant MFA • Privileged Access Management 	<ul style="list-style-type: none"> • Dark Web Monitoring • Vulnerability Scans 	<ul style="list-style-type: none"> • Awareness Training • Phishing Simulation
Compliance					

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

70



Compliance

- Regardless of your federal or state requirements...
- Compliance yields security
- What do your customers expect?
- People aren't waking up expecting to be in a breach.
- What does this mean?

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved. Source – Google Images / connectwise.com
Do not distributed without the written consent of Stasmayer, Incorporated.

71



Endpoint Security

Managed Detection and Response (MDR)

Endpoint Detection and Response (EDR) is an organizational security tool that monitors, detects, and responds to malicious activity on enterprise networks. It collects data from endpoints such as desktops, laptops, and mobile devices, which it then analyzes for suspicious activity likely to come from hackers. It responds to this suspicious activity by blocking it, alerting users, or taking other actions. EDR detects a range of activity, such as malicious code, malicious files, and network intrusions, and works by collecting system and network data, such as log files, network traffic, and memory dumps.

It becomes an MDR when it's connected to a 24/7 Security Operation Center (SOC).

Helps you fight against network attacks, ransomware, zero-day attacks, and insider

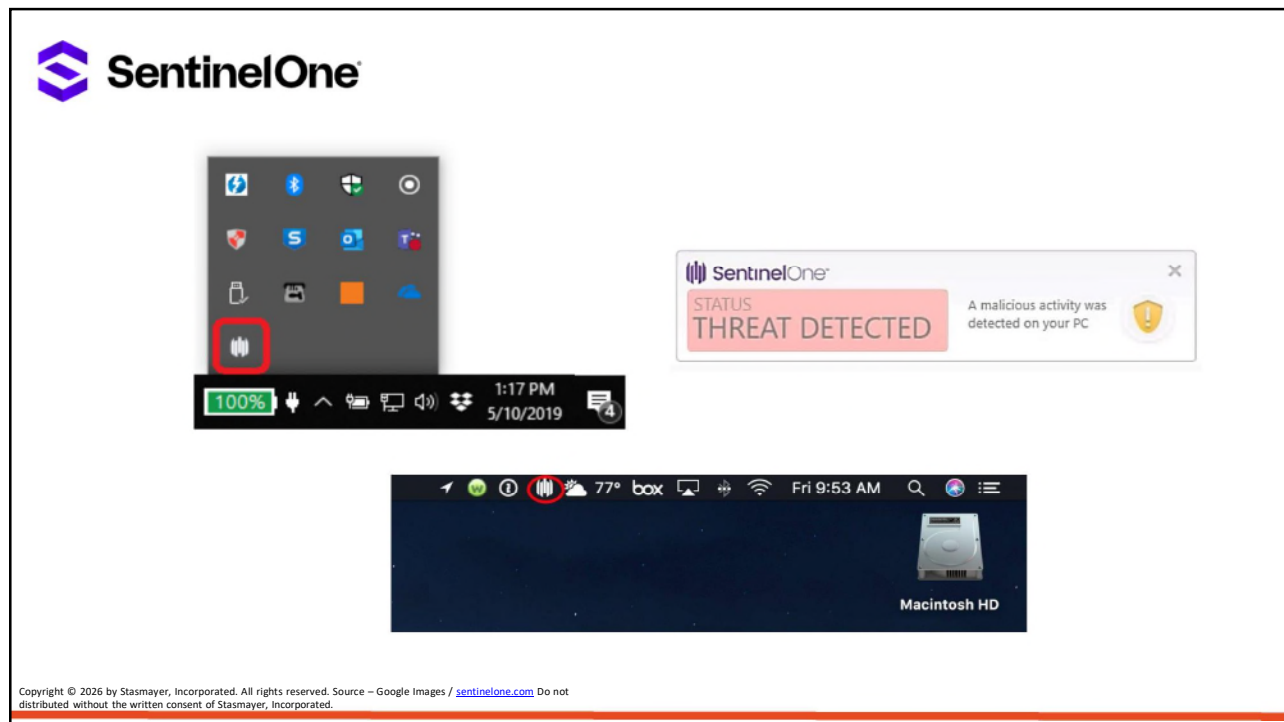
threats. Pricing varies based on vendor, options, and network environments.



Solo Law Firm Tip: If using Microsoft 365 Premium, Microsoft Defender for EDR is Included.

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved. Source – Google Images / connectwise.com
Do not distributed without the written consent of Stasmayer, Incorporated.

72



73

Threat Management

Security Information and Event Monitoring (SIEM)

Security Information and Event Management; SIEM is a co-managed threat detection and response platform that offers a powerful alternative to expand the security perspective of a business to both prevention and detection.

Lots of companies are bundling MDR and SIEM.

Pricing varies based on vendor, options, and network environments.

Solo Law Firm Tip: Rare that you will be required to have this.

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved. Source – Google Images / [connectwise.com](https://www.connectwise.com) Do not distributed without the written consent of Stasmayer, Incorporated.

74

New Save Open Share Inspect

Search KQ1 - 18 days ago • 17 days ago Refresh

1 **O365kertExce5s** value.pnreiturestorUser • Add filter

-office365-records 0 29 hits Nov 23, 2020 @ 10:02:00 000 - Nov 24, 2020 (010:02:00.000 - Auto S./

Selected fields


LogonError
t Operation

GC C.:

timestamp per 30 minutes

UserKey	Time	World	User	ExtorsOadPropartlem	LefesnError	CbentIP	Operation	tovent_type	parch_commminy_natme	gmodalcommery_ftwme
t event.W9	> Nov 24, 2020 • OQ 50 43 000	ryanOp erchse curit y.com	ryanOpe rchsecu rity.co m	('Value': *Nacv05*X/10.12.6 (16G erNameOrP assuord 29) CalendarAgent/366', 'Name': *UserAgent').)	InvalidUs erNameOrP assuord (16G 2.12.1 35	35.14 2.12.1 35	Userlogi nFatted	office365	Perch	United States
t geolp country-name	> Nov 24, 2020 • 09 31.51.000	ryanOp erchse curit y.cos	ryanipe rchsecu rity.co 0	('Value': *Nec+05*X/10.12.6 (166 erNameOrP assuord 29) CalendarAgent/306', 'Name': 'UserAgent')	InvalidUs erNameOrP assuord (166 2.12.1 35	35.14 2.12.1 35	Userlooi 7trailed	office365	Perch	United States
t per0tt_C0rtipariry_name	> Nov 24, 2020 0 09 14 43.000	ryanOp erchse curat y.com	ryanOpe rchsecu rity.co m	('Value': *Mac+05*X/10.12.6 (16G erNameOrP assuord 29) CalendarAgent/306', 'Name': 'UserAgent')	InvalidUs erNameOrP assuord (16G 2.12.1 35	35.14 2.12.1 35	UserLogt mailed	office365	Perch	United States
ExtetidedProperbes	> Nov 24, 2020 0 09 14 43.000	ryanOp erchse curat y.com	ryanOpe rchsecu rity.co m	('Value': *Mac+05*X/10.12.6 (16G erNameOrP assuord 29) CalendarAgent/306', 'Name': 'UserAgent')	InvalidUs erNameOrP assuord (16G 2.12.1 35	35.14 2.12.1 35	UserLogt mailed	office365	Perch	United States
Avartable hetes	> Nov 24, 2020 0 09 14 43.000	ryanOp erchse curat y.com	ryanOpe rchsecu rity.co m	('Value': *Mac+05*X/10.12.6 (16G erNameOrP assuord 29) CalendarAgent/306', 'Name': 'UserAgent')	InvalidUs erNameOrP assuord (16G 2.12.1 35	35.14 2.12.1 35	UserLogt mailed	office365	Perch	United States
Actor	> Nov 24, 2020 0 09 14 43.000	ryanOp erchse curat y.com	ryanOpe rchsecu rity.co m	('Value': *Mac+05*X/10.12.6 (16G erNameOrP assuord 29) CalendarAgent/306', 'Name': 'UserAgent')	InvalidUs erNameOrP assuord (16G 2.12.1 35	35.14 2.12.1 35	UserLogt mailed	office365	Perch	United States
ActorContextId	> Nov 24, 2020 0 09 14 43.000	ryanOp erchse curat y.com	ryanOpe rchsecu rity.co m	('Value': *Mac+05*X/10.12.6 (16G erNameOrP assuord 29) CalendarAgent/306', 'Name': 'UserAgent')	InvalidUs erNameOrP assuord (16G 2.12.1 35	35.14 2.12.1 35	UserLogt mailed	office365	Perch	United States
Act ocipAdress	> Nov 24, 2020 0 09 14 43.000	ryanOp erchse curat y.com	ryanOpe rchsecu rity.co m	('Value': *Mac+05*X/10.12.6 (16G erNameOrP assuord 29) CalendarAgent/306', 'Name': 'UserAgent')	InvalidUs erNameOrP assuord (16G 2.12.1 35	35.14 2.12.1 35	UserLogt mailed	office365	Perch	United States
ApplicationId	> Nov 24, 2020 0 09 14 43.000	ryanOp erchse curat y.com	ryanOpe rchsecu rity.co m	('Value': *Mac+05*X/10.12.6 (16G erNameOrP assuord 29) CalendarAgent/306', 'Name': 'UserAgent')	InvalidUs erNameOrP assuord (16G 2.12.1 35	35.14 2.12.1 35	UserLogt mailed	office365	Perch	United States
AzureAct tveDirectoryEve.	> Nov 24, 2020 0 09 14 43.000	ryanOp erchse curat y.com	ryanOpe rchsecu rity.co m	('Value': *Mac+05*X/10.12.6 (16G erNameOrP assuord 29) CalendarAgent/306', 'Name': 'UserAgent')	InvalidUs erNameOrP assuord (16G 2.12.1 35	35.14 2.12.1 35	UserLogt mailed	office365	Perch	United States
COMPANY	> Nov 24, 2020 0 09 14 43.000	ryanOp erchse curat y.com	ryanOpe rchsecu rity.co m	('Value': *Mac+05*X/10.12.6 (16G erNameOrP assuord 29) CalendarAgent/306', 'Name': 'UserAgent')	InvalidUs erNameOrP assuord (16G 2.12.1 35	35.14 2.12.1 35	UserLogt mailed	office365	Perch	United States

75



Threat Management

Identity Threat Detection and Response (ITDR)

ITDR continuously watches identity systems for **post-compromise behavior**, such as:

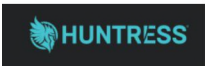


- Suspicious authentication
- Account takeover behavior in M365 / Google Workspace
- Cloud configuration changes

How ITDR relates to BEC (Business Email Compromise)

Business Email Compromise often looks like:

- User gets phished
- Attacker logs in (no malware)
- Attacker creates mail rules + sets up persistence
- Attacker impersonates and initiates wire fraud

ITDR is designed to catch steps **2-4**, even when the attacker is using valid credentials.

Solo Law Firm Tip: Microsoft Defender for Office 365 with Subscription + Entra ID

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved. Source – Google Images
Do not distributed without the written consent of Stasmayer, Incorporated.

76

Incident Response

Incident Response Policy & Plan

Great Resource - <https://www.hhs.gov/sites/default/files/cybersecurity-incident-response-plans.pdf>

Resource:

- Computer Security Incident Handling Guide Available - NIST SP 800-61 Revision 2
- Seeks to give organizations practical guidelines / Not regulatory documents
- Primary focus: Detecting, analyzing, prioritizing, and handling incidents

1. Make a Policy to define what is a security incident for your firm
2. Create Cybersecurity Incident Response Plan
3. Preparation and Planning
4. Training and Test



Solo Law Firm Tip: Easy

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved. Source – above link
Do not distributed without the written consent of Stasmayer, Incorporated.

77



Incident Response

Cyber Insurance

A key component to your Incident Response Plan

Find a Cyber Insurance Company that Specializes in Cyber Insurance which can help you cover:

1. 3rd Party Liability
2. Cyber Extortion
3. Business Interruption
4. Data Breach
 - Data breach response and remediation, including legal defense costs, customer, IT forensics, crisis media relations support and necessary work with regulators and authorities.

<https://datastreaminsurance.com/>



Solo Law Firm Tip: Easy

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved. Source – datastreaminsurance.com
Do not distributed without the written consent of Stasmayer, Incorporated.

78

Cyber Insurance Requirements



If you don't have cyber insurance, get it!



Could be de facto regulation requirements for you.



Requirements are valuable safeguards. GOOD THING!



Could be the best thing that happened to you.



Copyright © 2022 by Stasmayer, Incorporated. All rights reserved.
The content of this presentation is proprietary and confidential information of Stasmayer, Incorporated. It is not intended to be recorded in any way, copied, or distributed without the written consent of Stasmayer, Incorporated.

79

Incident Response

How it works

Insurance

Breach Coach

Forensics

Attorney Client Privilege

NEVER DO THEM ON YOUR OWN!

Report all crimes to <https://www.ic3.gov/>



Copyright © 2022 by Stasmayer, Incorporated. All rights reserved.
The content of this presentation is proprietary and confidential information of Stasmayer, Incorporated. It is not intended to be recorded in any way, copied, or distributed without the written consent of Stasmayer, Incorporated.

80



Secure Access

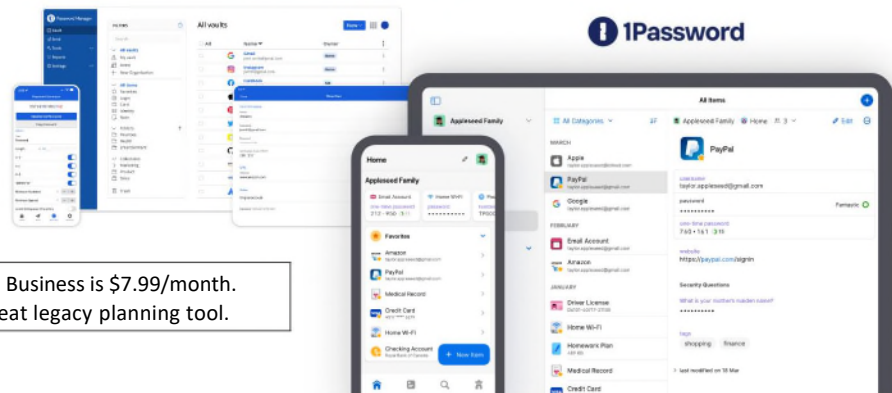
Password Management with Pass Key

Central Password Management for Personal, Family, Teams and Business

- Protect yourself
- Save time
- Actionable Insights
- Legacy Protection
- Can Log Activity with SIEM
- Be Used with SSO
- FIDO2 Keys



Pricing starts \$1/month and up depending on solution



Solo Law Firm Tip: 1Password Business is \$7.99/month. Can link with Entra ID. Great legacy planning tool.

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved. Source – 1password.com / bitwarden.com / yubico.com Do not distributed without the written consent of Stasmayer, Incorporated.

81



Secure Access

Phishing-resistant MFA Authentication

Phishing-resistant Multi-Factor Authentication (MFA) is like having an ultra-secure lock on your online accounts that requires not just a password, but also something unique to you (like your fingerprint or a special key) to unlock.

Do not use SMS, Voice, or Email for MFA

Pricing varies per vendor and network environment.



Solo Law Firm Tip: Microsoft Entra ID

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved. Source – okta.com / duo.com / [Microsoft.com](https://microsoft.com) Do not distributed without the written consent of Stasmayer, Incorporated.

82



Risk Assessment

Dark Web Monitoring

- Dark Web Monitoring is a service that scans for your personal and company information on dark websites and forums. It is important because identity thieves can buy or sell your personal information to commit several illicit activities.

Pricing varies per vendor.



Item	Info type	Source name	Breach	Price (\$USD)	Rank	Strong Identifier	Report date
Credit Cards for Sale (3,448)							
Bit Data for Sale (23,528)							
Black Markets (84,790)							
	CW		28,12 mix...	10.0		Not exposed	Dec 29, 2021
	CW		28,12 mix...	10.0		Not exposed	Dec 29, 2021
	CW		28,12 mix...	10.0		Not exposed	Dec 29, 2021
	CW		28,12 mix...	10.0		Not exposed	Dec 29, 2021
	CW		28,12 mix...	10.0		Exposed	Dec 29, 2021

Solo Law Firm Tip: www.havebeenpwned.com

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved. Source – [Norton.com/rapid7.com/google images/](https://norton.com/rapid7.com/google-images/) Do not distributed without the written consent of Stasmayer, Incorporated.

83



Risk Assessment

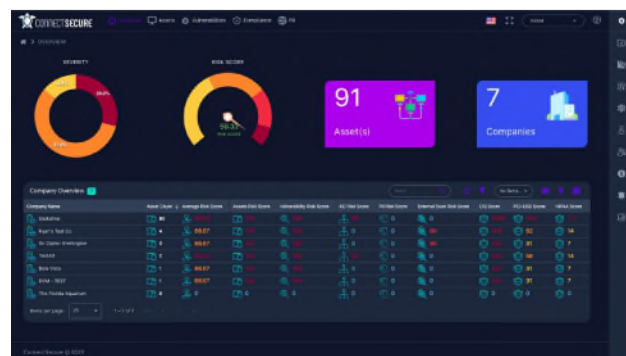
Vulnerability Scans

Proactively identify and address security weaknesses, reducing the risk of cyberattacks and potential data breaches.

Ensure that software vulnerabilities are promptly addressed, minimizing the risk of security breaches and protecting valuable data.



Solo Law Firm Tip: M365 Premium (lacks external networking scans / pen testing)



Copyright © 2026 by Stasmayer, Incorporated. All rights reserved. Source – connectsecure.com/rapid7.com/tenable.com/rapidfiretools.com Do not distributed without the written consent of Stasmayer, Incorporated.

84



Training

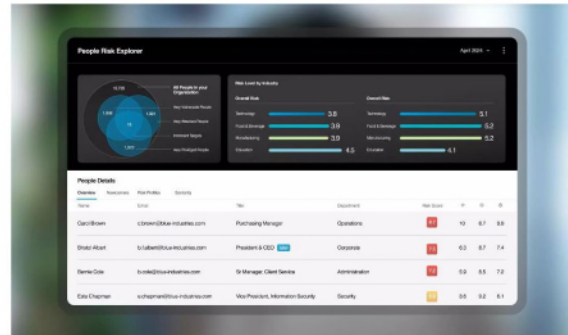
Awareness Training

Training is #1 when it comes to Cybersecurity.

Solutions include:

- Attack vector training
- Behavioral Science
- Training Reports
- Phish Reporting
- And more...

Pricing varies per vendor, options and user requirements.



Solo Law Firm Tip: www.cisa.gov – Free Training

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved. Source – ninjo.com/knowbe4.com/proofpoint.com Do not distributed without the written consent of Stasmayer, Incorporated.

85



Training

Phishing Simulation

- Test your staff after training and often
- Not a one and done
- Automated simulation
- Super Valuable

Pricing varies per vendor, options and user requirements.

The screenshot shows the 'Create New Phishing Campaign' form in the KnowBe4 interface. The form includes fields for Name, Email To, Frequency, Start Time, and various checkboxes for sending and tracking. The 'Name' field is set to 'My first phishing campaign'. The 'Email To' field is set to 'Accounting'. The 'Frequency' is set to 'One time'. The 'Start Time' is set to '09:00:00'. The 'Send' checkbox is checked. The 'Track Activity' checkbox is also checked. The 'Categories' dropdown is set to 'IT'. The 'Phase Link Domain' is set to 'Random'. The 'Landing Page' is set to 'User Defaults'. The 'Add External' dropdown is set to 'None'. The 'Add Clicked To' dropdown is set to 'Clickers'. The 'Send an email report to account admin after each Phishing Security Test' checkbox is checked.



Solo Law Firm Tip: www.knowbe4.com/free-cybersecurity-tools/phishing-security-test

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved. Source – ninjo.com/knowbe4.com/proofpoint.com Do not distributed without the written consent of Stasmayer, Incorporated.

86



#1 Step – If you Click Something

- 1. Unplug the Device**
- 2. Tell your IT to Isolate and Air Gap**
- 3. Call your Cyber Insurance Carrier Immediately**

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

87



Lightning Round

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

88

Protect your wire transactions!

- Verify Identity and Bank Details
- Wire Fraud Insurance
- Fraud Recovery Services

Contact for pricing

<https://www.certifid.com/>

WIRE FRAUD PROTECTION

"I didn't think it could happen to me."

During a real estate transaction, 1 in 4 consumers and businesses are targeted for wire fraud. Prepare and don't fall for it yourself.

Request a Demo

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

89

Wi-Fi Pineapple

Looks like a Router! It' not!


- Helps user create a Rogue Access Point
- Steal People's Login Credentials
- Carry out Advanced man-in-middle attacks
- Analyze Wi-Fi Handshakes
- Crack Wi-Fi passwords
- And more....

\$139.99

[https://shop.hak5.org/p](https://shop.hak5.org/products/wifi-pineapple) rodu cts/wifi-pineapple

Example
SSID: 2026SCBARCLECenter

Source: <https://www.zdnet.com/article/7-hacking-tools-that-look-harmless-but-can-do-real-damage/>



Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

90



Security News



Latest news on security and breaches

Go to krebsonsecurity.com to subscribe

Free

Source: krebsonsecurity.com

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated

91



- SANS is the most trusted and by far the largest source for information security training and security certification.
- Free Resources - Policies ranging from Acceptable Use, Email Policy, Password Protection, and more

<https://www.sans.org>

<https://www.sans.org/information-security-policy/?msc=securityresourceslp>

Source: [sans.org](https://www.sans.org)



Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated

92

Flipper Zero

Pen-testing Swiss Army Knife

- Built in transceiver, antennas, iButton/NFC/RFID reader/writer/emulator, and more
- Control items that have infrared remotes, clone RIF cards and NFC tags, capture and retransmit radio frequencies
- Access Lock Cars, send keystrokes, unlock doors with badges,



\$169

<https://shop.flipp erzero.one/>

Source: <https://www.zdnet.com/article/7-hacking-tools-that-look-harmless-but-can-do-real-damage/>

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

93

O.MG cables

Charging Cables with a Computer!

- Remote operator can do anything
- Steal Wi-Fi passwords
- Copy and Delete Files
- Plant Spyware and Malware
- Can be programmed to self-destruct



\$199

<https://shop.hak5.org/products/omg-cable>

Source: <https://www.zdnet.com/article/7-hacking-tools-that-look-harmless-but-can-do-real-damage/>

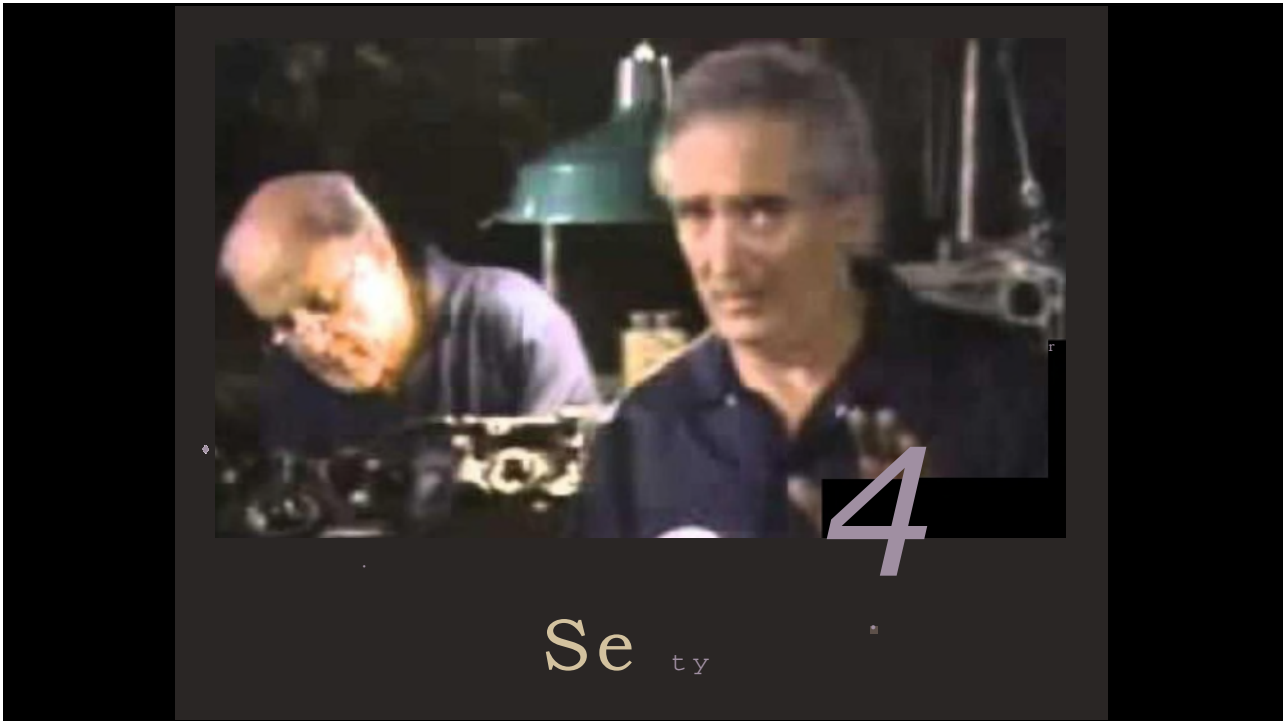
Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

94

Last Inning

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

95



96



97



98



We believe organizations need to make cybersecurity a community and training effort.

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

99



But by not mentioning it....the legal community is not benefiting.

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

100



Alert: Fraudulent email messages from SCBAR

Like
This!

Alert! Phishing emails—June 22 and 24, 2022

Fraudulent email messages were sent to some members of the SC Bar on June 22 and June 24 with the subject lines "Support Jack" and "Bobs Campaign." If you received these fraudulent emails, delete and do not click on links.

While the messages said they were from "The South Carolina Bar," both came from gmail.com addresses.

Unfortunately, phishing attacks are on the rise, and cyber criminals behind such messages are becoming increasingly clever in ways to get past filters and into your inboxes including using logos and organization names.

Note, these types of phishing messages do not mean the SC Bar has been hacked. Phishing is a way cyber criminals **masquerade as a trustworthy source** in an attempt to bait a user to surrender sensitive information such as a username, password, credit card number, etc.

Protect yourself and your information by always looking carefully at your email messages. Don't trust the display name (whether it's SC Bar or South Carolina Bar). Fraudsters will spoof both company/organization names and display names, and often hijack legitimate logos. Please read more tips about spotting phishing messages and protecting yourself.

- Check the message body for **spelling and punctuation mistakes and strange phrases**.
- **Beware of urgent calls to action or threats of penalty.** Be highly suspicious of emails that say you must click a link or open an attachment immediately. Creating a false sense of urgency is a common trick of phishing attacks and scams.
- **Look at the body of the email but don't click links or open attachments.** Never open an attachment in a message that you are not expecting to receive.
- **Don't give any personal information.** The SC Bar and all legitimate companies/organizations will **not** ask for personal information via email.
- **Remain vigilant.** Phishers are very good at what they do, and most malicious messages now contain convincing brand logos, language, titles of key leaders and email addresses that **may** look valid. Be skeptical when reading your email messages. If you receive a message from the SC Bar that appears to be suspicious, please contact us

Thank you to the Bar members who alerted us to this message.

Source - <https://www.scbars.org/bar-news/article/alert-fraudulent-email-message/>

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

101

Let's Build a Stronger Community



Copyright © 2026 by Stasmayer, Incorporated. All rights reserved. Source - [_hp-habitat-for-hu-manity.jpg \(1019x673\) \(thegoodbeginning.com\)](#) - This Photo by Unknown Author is licensed under CC BY Do not distributed without the written consent of Stasmayer, Incorporated.

102



Please keep this in mind...

- We sometimes get calls from people in tears.
- This has already happened to your peers.
- And...most of them don't talk about it.

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

103

Please take security seriously.

Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

104



Thank you for your time. Questions?

Want a Free Security Checklist - info@stasmayer.com

Rick Krenmayer – rick@stasmayer.com

David Stasaitis – dave@stasmayer.com

Stasmayer, Incorporated
3815 W. Montague Ave, Suite 200
North Charleston, SC 29418
Office Phone: 843-724-3440

www.stasmayer.com



Copyright © 2026 by Stasmayer, Incorporated. All rights reserved.
Do not distributed without the written consent of Stasmayer, Incorporated.

105

THE END

106



South Carolina Bar

Continuing Legal Education Division

**Systemize the Work, so you can Be the Lawyer:
Real tools. Real workflows. Real time back**

Brooks Derrick

No Materials Available