

The Paradox of Ethical Lying

Turning a Hackers Tricks into your Tactics

Copyright © 2025 Secure Ideas LLC

What's one word you associate with lying?



Copyright © 2025 Secure Ideas LLC

Kathy Collins

Security Consultant Secure Ideas, LLC

- Secure Ideas since 2021
- Based in Jacksonville, Florida
- CISSP, PCIP

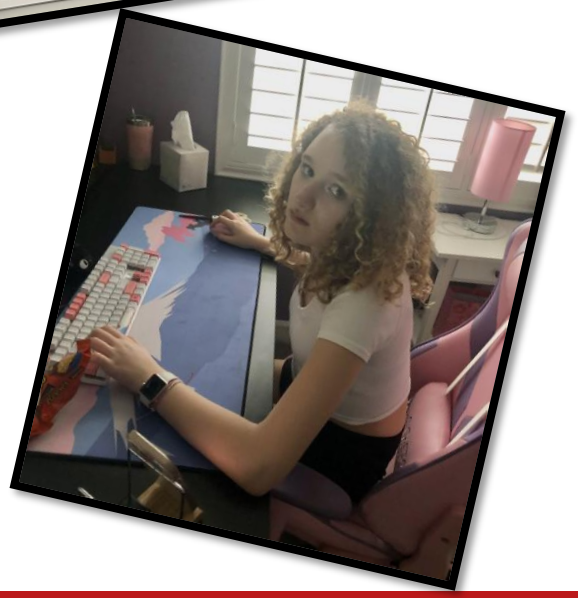
Focus Areas

- Networks
- Web Applications
- PCI DSS
- Physical Pentesting

Other Fun Facts

- Former Chef
- Mother of doggos (and a teenager)
- Horror Nerd
- BSides Jacksonville Coordinator
- Costco Member

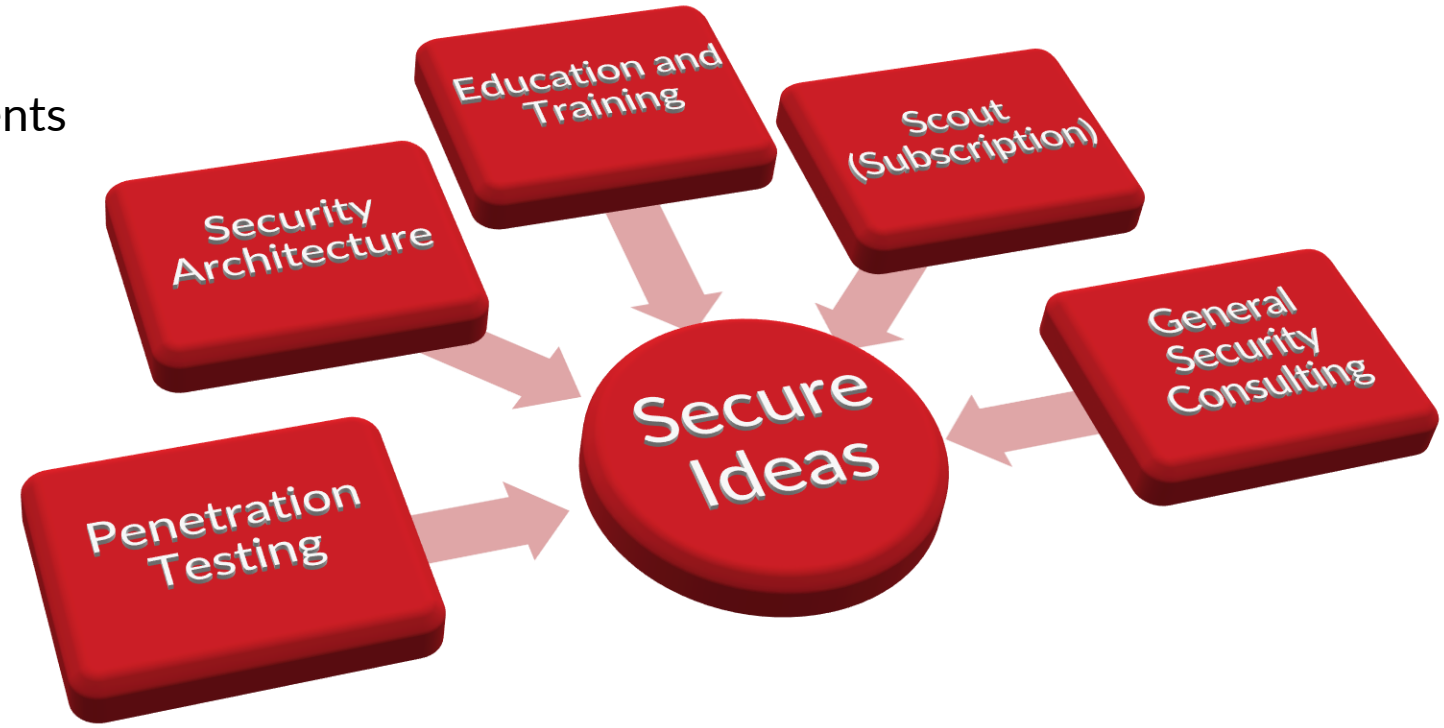




Copyright © 2025 Secure Ideas LLC

About Secure Ideas

- Founded in September 2010
  - Kevin Johnson: CEO, former SANS instructor and author
- Based in Jacksonville, FL
  - Consultants live around the country
- Expert Security Consultants
  - Penetration Testing & Vuln Assessments
  - Security Architecture Reviews
  - Education (training, conference talks)
- "Security Evangelists"
  - Open Source authors/contributors
  - Blogs (blog.secureideas.com)
  - "Heart of a Teacher"



Copyright © 2025 Secure Ideas LLC

What is "Professionally Evil"?

professionally evil®

We need to think "evil" so we can understand **how** an attacker will behave and **what** they will attack.

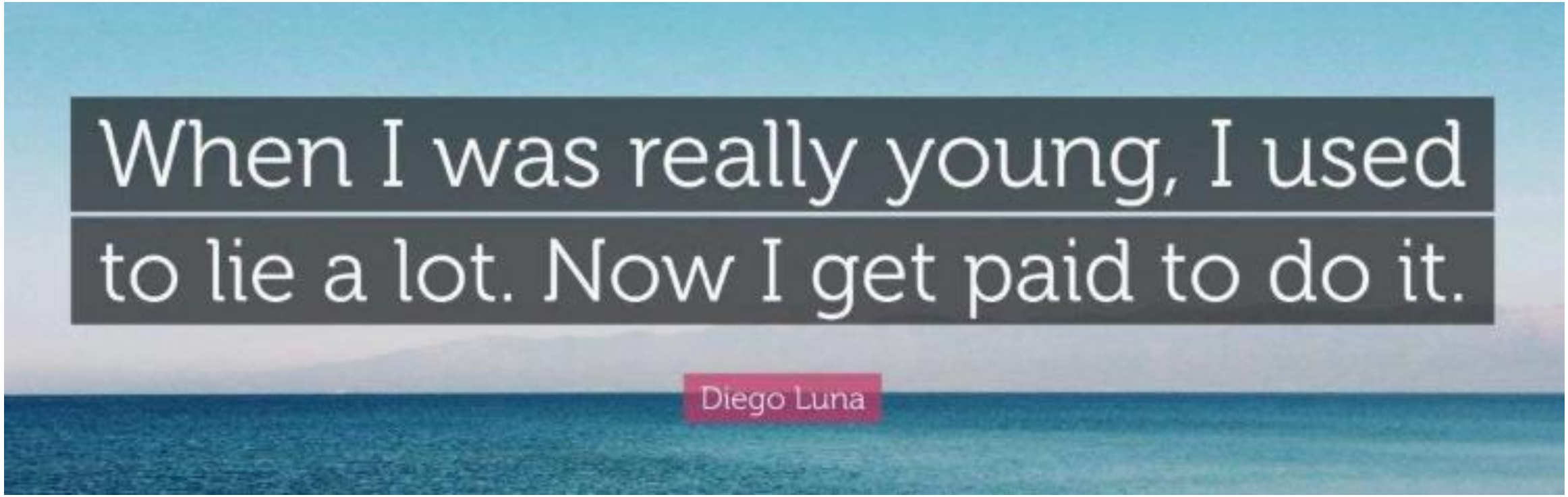
And we are Professional:

- Help companies improve their security posture
- Permission: Penetration Testing is always under contract
- Establish and follow rules of engagement



Copyright © 2025 Secure Ideas LLC

The Ethical Liars Dilemma



Copyright © 2025 Secure Ideas LLC

Deception as a Defensive Strategy



Lying with Permission

Controlled Misinformation

Exposing Weaknesses

Teaching with Trickery

Copyright © 2025 Secure Ideas LLC

The Paradox Defined



Copyright © 2025 Secure Ideas LLC

Security vs. Integrity

Data integrity



The degree to which data is **unimpaired**.

Data security



The degree to which data is **protected**.

Copyright © 2025 Secure Ideas LLC

The Subpoena Evasion Coupon



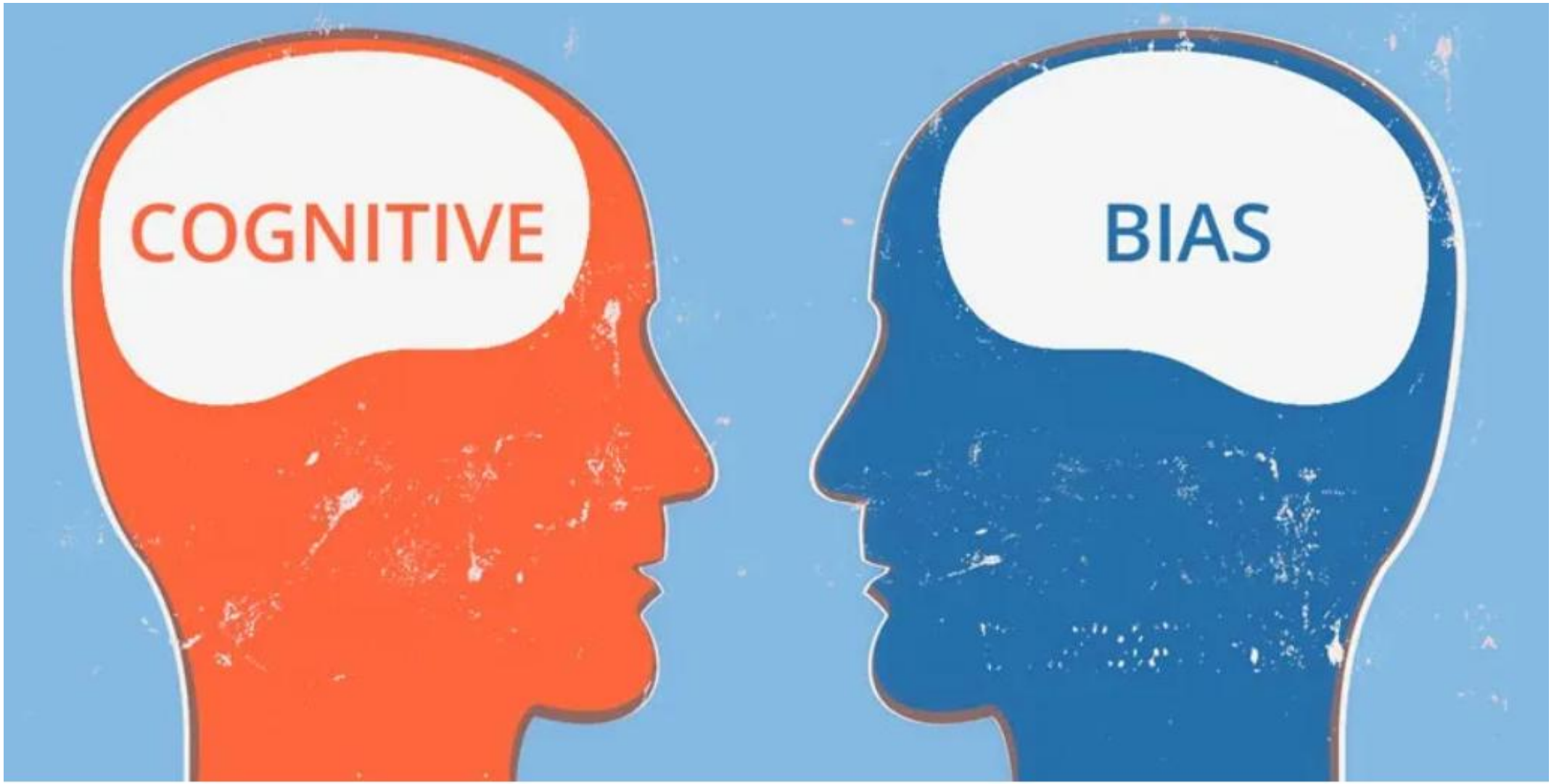
Copyright © 2025 Secure Ideas LLC

History of Social Engineering

Early 1900s:	Face-to-face scams and classic confidence tricks
1940s–1970s:	Emotional manipulation, fear tactics, and early impersonation
1980s–1990s:	Phishing emails and fake websites take off; VoIP opens the door to caller ID spoofing
2000s–2010s:	Spear phishing, social engineering tests, and business email compromise explode
2020s–Today:	AI, deepfakes, and automation fuel hyper-personalized scams across platforms

Copyright © 2025 Secure Ideas LLC

Default Brain Settings



Copyright © 2025 Secure Ideas LLC

Authority



- People trust perceived authority figures
- Attackers spoof authority figures
- Victims comply without verifying

Copyright © 2025 Secure Ideas LLC

Urgency

- **Pressure to act fast overthrows caution**
- ***Your account will be locked in two minutes!***
- **Speed becomes more important than security or accuracy**



Copyright © 2025 Secure Ideas LLC

Familiarity



- We tend to trust people who seem like "one of us"
- Attackers mimic people you know
- Familiar language also lowers defenses

Copyright © 2025 Secure Ideas LLC

Reciprocity

- "I owe you one" can be powerful
- Fake help or small favors
- We feel compelled to return the favor



Copyright © 2025 Secure Ideas LLC

Break Time



Copyright © 2025 Secure Ideas LLC

The Hackers Tackle Box



Copyright © 2025 Secure Ideas LLC



Why we like it

- Free and legal
- Builds context
- It makes it easier!
- Informed targeting

What is it

- LinkedIn
- Company Websites
- Social Media
- Github
- Pastebin
- Breach Forums
- Search Engines
- Google Dorking

Copyright © 2025 Secure Ideas LLC

The RUSE

- **Phishing**
  - *Official or curious emails*
- **Vishing**
  - *Employee, tech support, HR*
- **Pretexting**
  - *The backstory*
- **Baiting**
  - *Tempting someone*



Copyright © 2025 Secure Ideas LLC

The PHYSICAL World



- Tailgating
- Impersonation
- Lockpicking
- USB Drops
- Low Tech Access

Copyright © 2025 Secure Ideas LLC

When the Ruse Becomes the Crime



Copyright © 2025 Secure Ideas LLC

MGM Resorts (Sept 2023)

- Vishing Attack on Help Desk
- Impersonation of Employee
- LinkedIn Profile
- Approved an MFA reset
- Gained Admin Access
- Ransomware Deployed
- Casino Meltdown
- $100 Million



Copyright © 2025 Secure Ideas LLC

Toyota Boshoku Corporation (Aug 2019)

Discovery of European subsidiary being subject of fraud

Kariya (JAPAN) -September 6, 2019- Toyota Boshoku Corporation (TOKYO:3116) announce a recent case involving fraudulent payment directions from a malicious third party that has resulted in a financial loss at our European subsidiary.

Together with the European subsidiary, we became aware that the directions were fraudulent shortly after the leakage. Recognizing the high possibility of criminal activity, we promptly established a team comprising legal professionals, then reported the loss to local investigating authorities. While cooperating in all aspects of the investigation, we are devoting our utmost efforts to procedures for securing/recovering the leaked funds.

We will promptly disclose any amendments to the released March 2020 earnings forecast if this incident makes such revision necessary.

Copyright © 2025 Secure Ideas LLC

Whatever Attackers Do, You Can Do Better





Phishing → Simulated Phishing Drills



Pretexting → Call-Back Verification



OSINT → Digital Footprint Checks



Tailgating → Physical Access Audits

Copyright © 2025 Secure Ideas LLC

Anti-Fraud Tacklebox



MULTI-STEP VERIFICATION



BEHAVIOR BASED TRAINING



CREATE A CULTURE OF PAUSE



INCIDENT SIMULATIONS

Copyright © 2025 Secure Ideas LLC

Questions?



Kathy.Collins@secureideas.com

@k4ffeine.bsky.social

twitter.com/K4FFEINE

linkedin.com/in/kathyvcollins/

Copyright © 2025 Secure Ideas LLC