Personal Cyber Security in an AI-Driven World

Kenneth G. Hartman

December 9, 2024

Grand Traverse Humanists

About Me

LUCID TRUTH TECHNOLOGIES
LucidTruthTechnologies.com

Kenneth G. Hartman

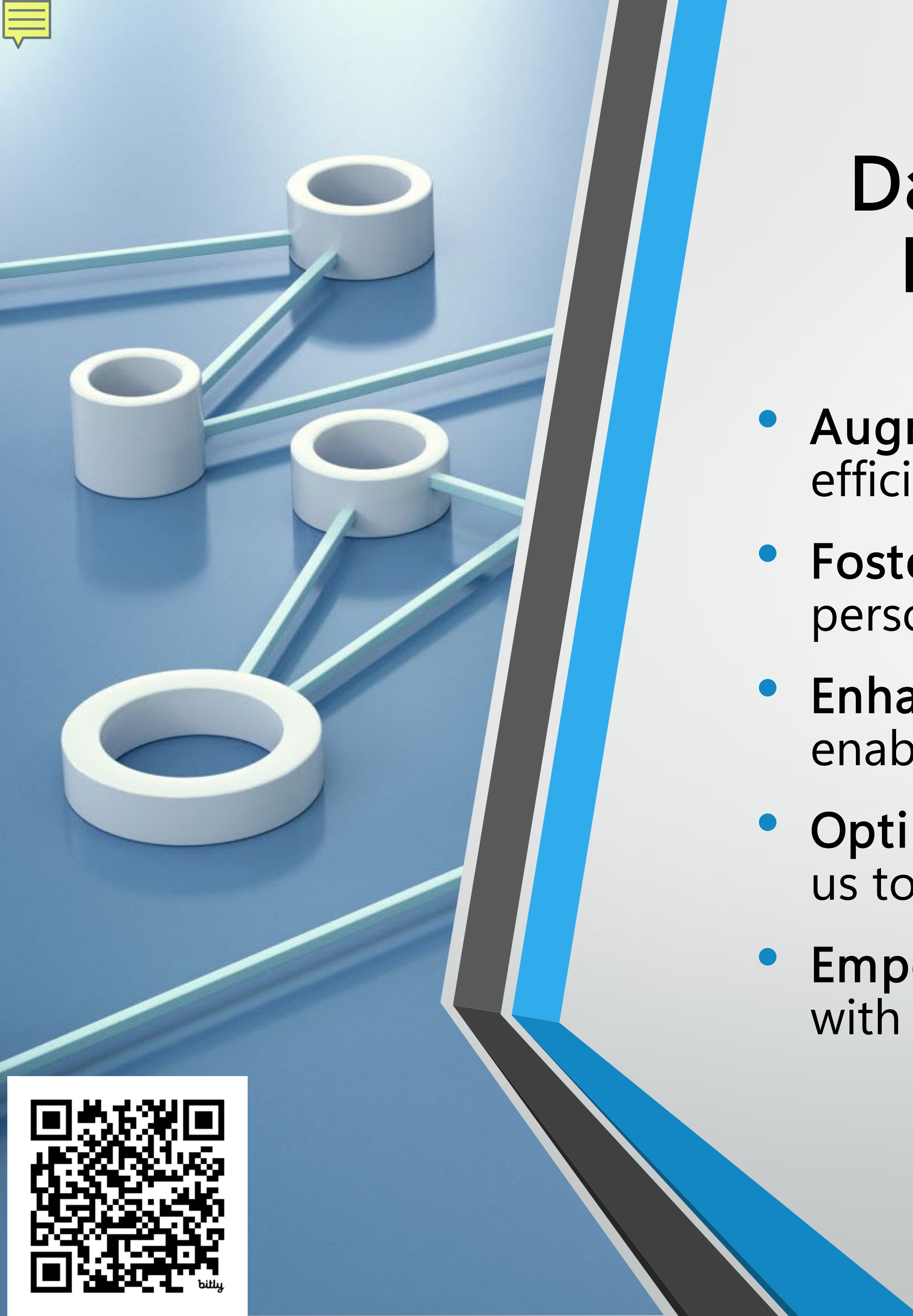
- Owner – Lucid Truth Technologies, a Digital Forensics Firm
- BS Electrical Engineering, Michigan Technological University
- MS Information Security Engineering, SANS Technology Institute
- Multiple Security Certifications: CISSP, GIAC Security Expert, etc.
- SANS Instructor – SEC488: Cloud Security Essentials
  & SEC510: Public Cloud Security: AWS, Azure, and GCP

www.kennethghartman.com
@kennethghartman

The content and opinions in this presentation are my own and do not necessarily reflect the positions, strategies, or opinions of any current client or previous employer.

A Humanist Lens on AI and Cybersecurity

- **Shared Goal:** Finding meaning and connection amidst technological change.
- **The Challenge:** Navigating risks posed by AI-driven cyber threats.
- **The Opportunity:** Empowering ourselves with knowledge and tools.
- **Tonight's Focus:**
    - Emerging threats: AI-powered scams, phishing, and voice cloning.
    - Practical protections: Multi-Factor Authentication (MFA), recognizing scams, and securing data.
    - Humanist perspective: Flourishing through understanding and critical thinking.



Daniel Miessler’s Take: How AI Can Help Us Become Better Humans

- **Augment Human Capabilities**: AI can enhance our skills, efficiency, and decision-making.
- **Foster Self-Improvement**: Tools like Human 3.0 aim to support personal growth and purpose-driven lives.
- **Enhance Understanding**: AI can simplify complex issues, enabling informed discussions and collaborative solutions.
- **Optimize Daily Life**: By automating mundane tasks, AI allows us to focus on creativity, relationships, and meaningful pursuits.
- **Empower Ethical Choices**: AI can guide us in aligning decisions with our values, fostering human flourishing.

TRUST

Trust in a Human Context

Reliance on others to act honestly, predictably, and align with shared expectations.

Key Characteristics:

- **Vulnerability**: Openness to risk of disappointment.
- **Consistency**: Built through reliable actions over time.
- **Reciprocity**: Mutual trust fosters stronger relationships.
- **Repairability**: Can be rebuilt with accountability and effort.

Types of Trust:

- **Interpersonal**: Between individuals (e.g., friends, partners).
- **Institutional**: In organizations or systems.
- **Cultural**: Based on shared community values.

Trust in Cybersecurity

Trust determines access for users, devices, or systems, relying on verification.

Key Characteristics:

- **Verification:** Credentials and authentication.
- **Least Privilege:** Minimal necessary access.
- **Zero Trust:** Continuous validation of all entities.
- **Resilience:** Designed to withstand breaches.

Mechanisms: Authentication, encryption, trust frameworks, and monitoring.

Breakdowns: Data breaches, phishing, and malware attacks.

Parallels Between Human and Cybersecurity Trust

Foundation in Relationships:

Human trust depends on personal connections; cyber trust depends on connections between systems, devices, and users.

Vulnerability:

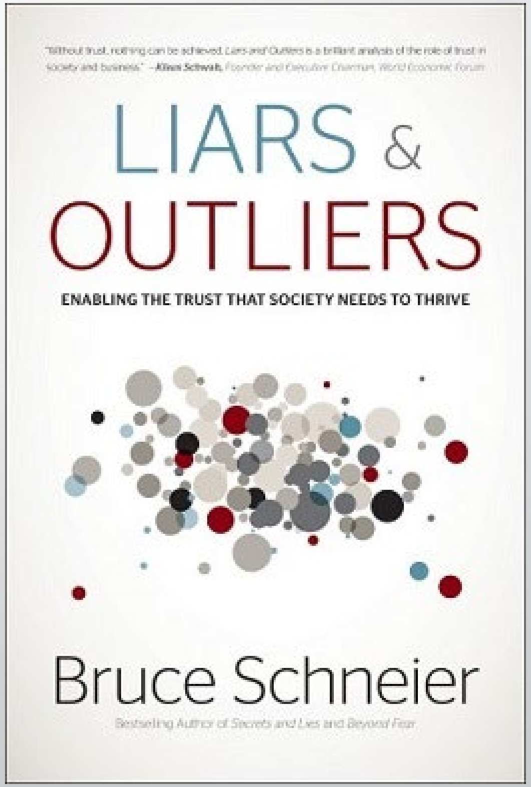
Humans take risks by trusting others, just as cybersecurity systems take calculated risks in granting access.

Betrayal and Recovery:

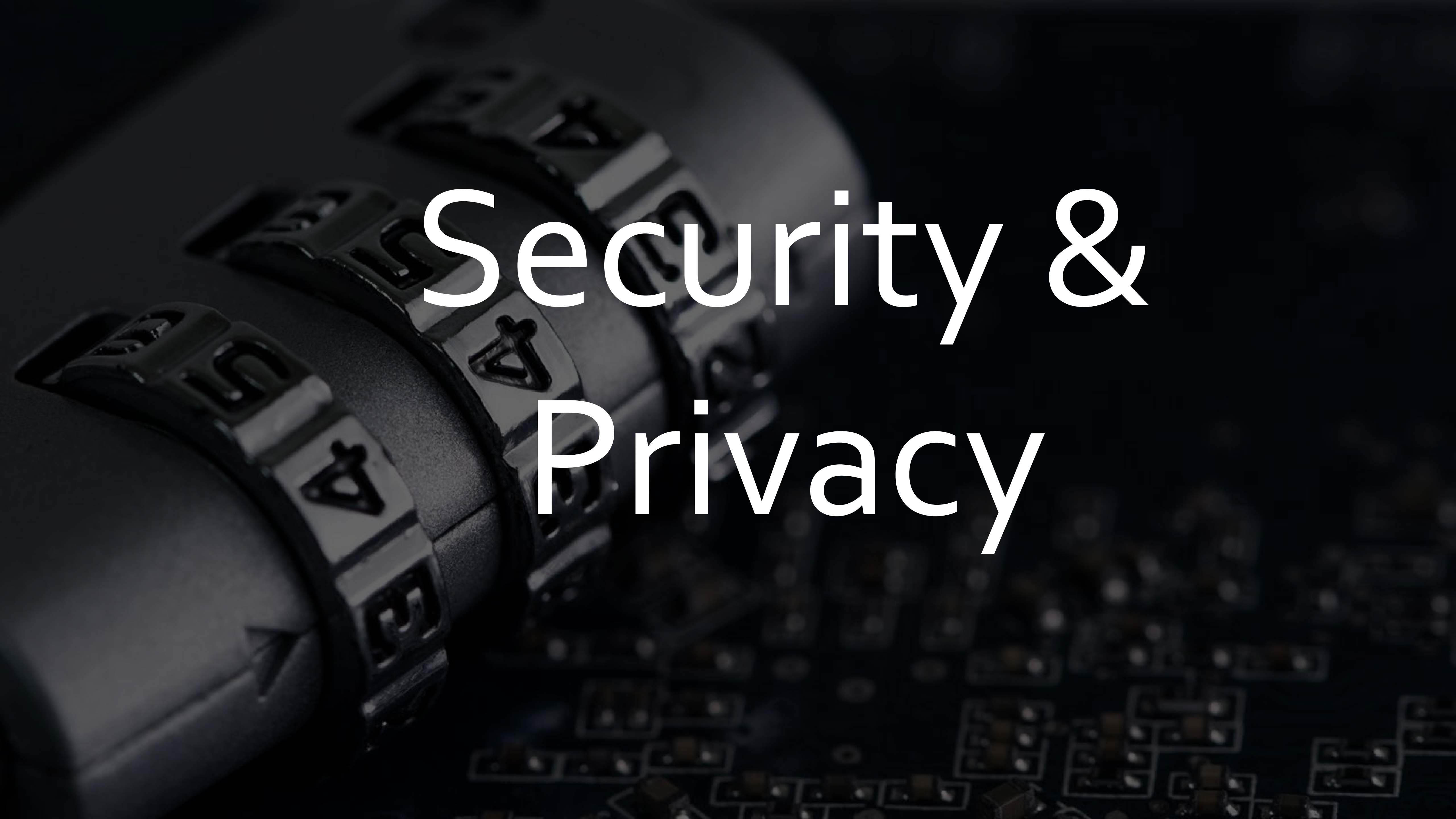
Trust can be broken and rebuilt in both domains, though cyber trust may involve patches, updates, or redesigned protocols, while human trust requires emotional work.

Bridging the Two Contexts

- **Human Weakness in Cybersecurity:** Many cybersecurity breaches exploit the human element of trust, such as employees clicking on phishing links or falling for scams.
- **Building Resilience:** Just as humans strengthen trust through communication and consistency, cybersecurity systems adopt models like “zero trust” to continually validate relationships without assumption.
- **Education and Awareness:** In both contexts, fostering trust requires knowledge—understanding risks, responsibilities, and tools for managing vulnerabilities.


"Without trust, nothing can be achieved. Liars and Outliers is a brilliant analysis of the role of trust in society and business." –Klaus Schwab, Founder and Executive Chairman, World Economic Forum
LIARS & OUTLIERS
ENABLING THE TRUST THAT SOCIETY NEEDS TO THRIVE
Bruce Schneier
Bestselling Author of Secrets and Lies and Beyond Fear

Security & Privacy



The CIA Triad: Foundations of Cybersecurity

Confidentiality: Protecting information from unauthorized access, like safeguarding personal privacy.

Integrity: Ensuring data is accurate and unaltered, reflecting honesty and truth.

Availability: Making information accessible when needed, aligning with open access to knowledge.

The CIA Triad mirrors humanist values—privacy, authenticity, and accessibility—ensuring the trustworthiness and usability of information in a connected world.

Privacy vs. Security: Key Differences

- **Privacy**: Protects personal information from being accessed or shared without consent. <u>It's about control over your data</u>.

- **Security**: Protects systems and data from unauthorized access or harm. <u>It's about safeguarding against threats</u>.

Privacy is the goal; security is the means to achieve it.

Both are essential for building trust in the digital world.

The Importance of Controlling Your Data

- **Preserves Autonomy**: You decide who can access and use your information.
- **Protects Privacy**: Safeguard personal details and identity from exposure.
- **Prevents Exploitation**: Minimize risks like fraud, manipulation, and data misuse.
- **Fosters Trust**: Encourages safer participation in digital spaces.
- **Promotes Accountability**: Pushes organizations to act ethically and transparently.

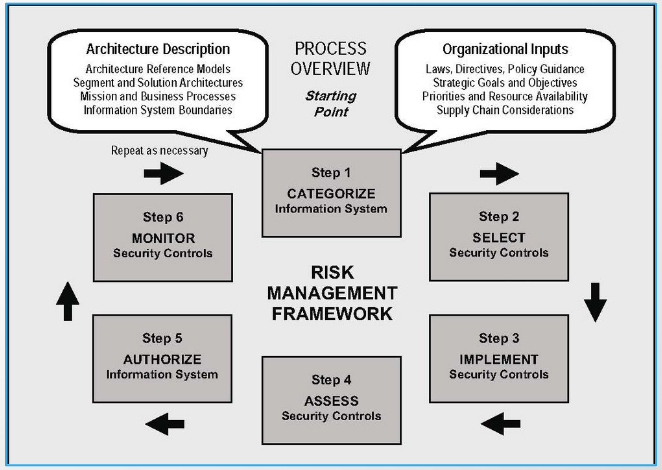
How to Exercise Control Over Your Data

- **Read Terms of Service:** Understand what you're agreeing to.
- **Use Privacy Tools:** Choose platforms like Signal and DuckDuckGo.
- **Limit Sharing:** Share only necessary information online.
- **Enable Security:** Use encryption, strong passwords, and MFA.
- **Support Regulations:** Advocate for privacy laws like GDPR and CCPA.

Risk Management

[redacted]

Key Principles of Risk Management


Architecture Description
Architecture Reference Models
Segment and Solution Architectures
Mission and Business Processes
Information System Boundaries
PROCESS OVERVIEW
Starting Point
Organizational Inputs
Laws, Directives, Policy Guidance
Strategic Goals and Objectives
Priorities and Resource Availability
Supply Chain Considerations
Repeat as necessary
Step 1 CATEGORIZE Information System
Step 2 SELECT Security Controls
Step 3 IMPLEMENT Security Controls
Step 4 ASSESS Security Controls
Step 5 AUTHORIZE Information System
Step 6 MONITOR Security Controls
RISK MANAGEMENT FRAMEWORK

Identify Risks: Recognize potential threats and what is at stake.

Assess Impact: Evaluate the consequences if a risk materializes.

Mitigate Risks: Use security controls to reduce vulnerabilities and prevent harm.

Monitor and Adapt: Continuously evaluate risks and update strategies as needed.

Balance Risk and Benefit: Ensure protective measures align with organizational or personal goals.

What Is a Security Control?

A security control is any measure or mechanism designed to **reduce** risks and protect assets from threats.

Purpose: Helps ensure confidentiality, integrity, and availability of data or systems.

Types:

- **Preventive**: Stops threats (e.g., firewalls, MFA, encryption).
- **Detective**: Identifies threats (e.g., monitoring systems).
- **Corrective**: Mitigates damage (e.g., backups, incident response).

Key Role: Security controls form the foundation of effective risk management.

There are no "perfect" security controls

Trust and Risk Management

Trust in Security Controls:

- Security controls must be reliable and effective to reduce risks.
- Trust builds when controls consistently perform as expected.

Risk vs. Blind Trust:

- Over-trusting controls without understanding limitations increases vulnerabilities.
- Regular testing and updates are essential to maintain trust.

Balancing Trust and Vigilance:

- Trust controls to manage risks but remain vigilant for failures or bypasses.
- Combine multiple layers of controls (defense in depth) to enhance protection.

Key Principle: Trust but verify—proactive oversight ensures robust risk management.

Understanding Vulnerabilities: Cybersecurity and Human Relationships

Cybersecurity Vulnerability:

A weakness in a system that can be exploited by attackers (e.g., outdated software, weak passwords).

Human Vulnerability:

In relationships, vulnerability is openness to trust, which can be exploited if met with dishonesty or betrayal.

Parallels:

Both require careful management—patching software in cybersecurity and fostering honesty and communication in relationships.

Awareness of vulnerabilities helps build resilience and trust in both contexts.

Social Engineering

Social Engineering: Exploiting Trust and Vulnerabilities

Manipulating people into revealing information or performing actions that compromise security.

Exploiting Trust:

- Attackers pose as trusted entities (e.g., impersonating a colleague or official).
- Relies on human nature to trust familiar roles or urgent requests.

Targeting Vulnerabilities:

- Weaknesses like lack of awareness or emotional triggers (e.g., fear, curiosity).

Bypassing Security Controls:

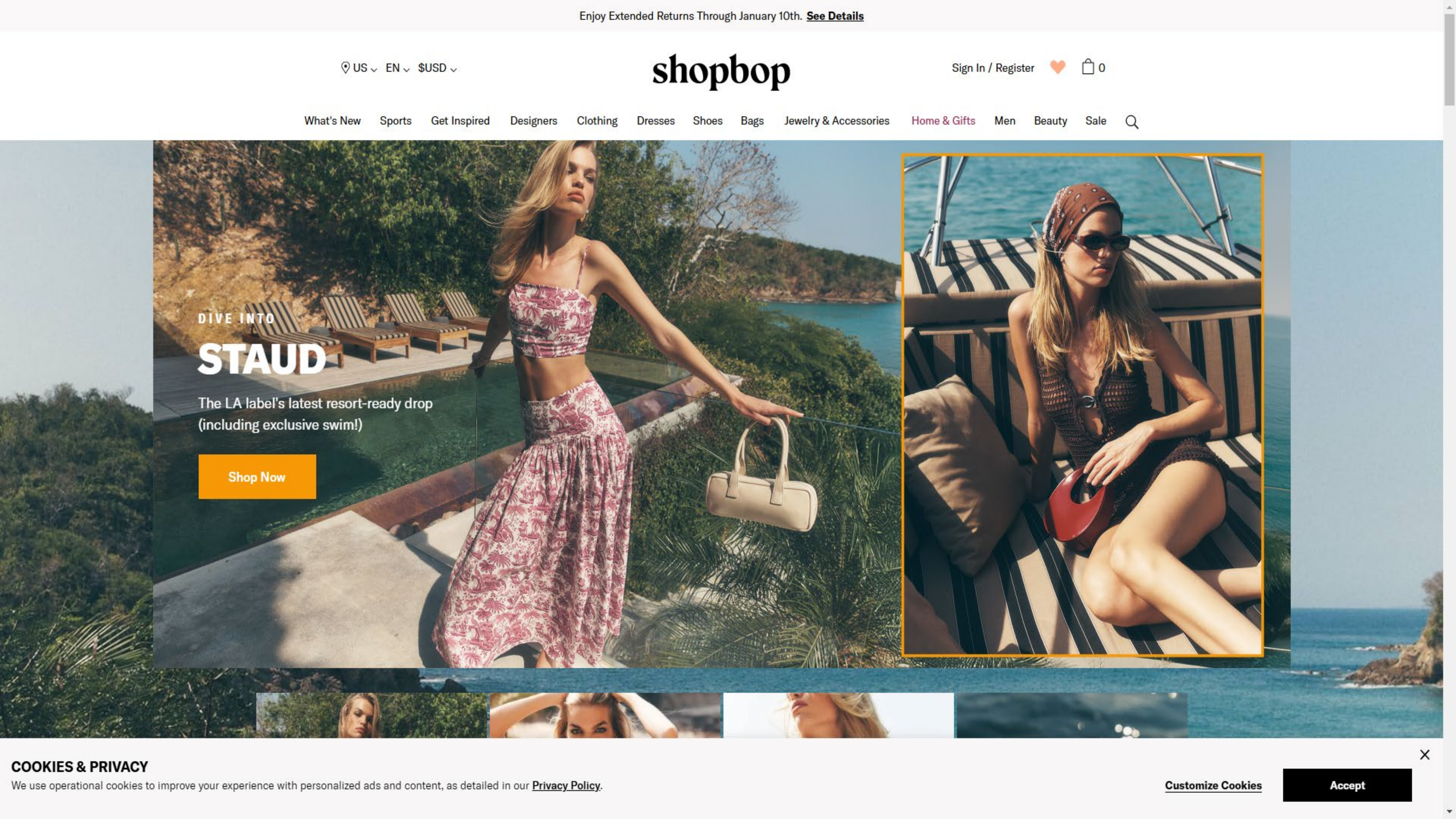
- Social engineering often exploits the human element, circumventing technical safeguards like MFA.

Phishing: A Form of Social Engineering

Phishing is a social engineering attack where cybercriminals trick individuals into sharing sensitive information or performing harmful actions by impersonating trusted entities.

- **Email Phishing**: Fake emails urging recipients to click malicious links or provide credentials.
- **Spear Phishing**: Highly targeted phishing aimed at specific individuals using personalized details.
- **Smishing**: Phishing through SMS messages with fraudulent links or requests.
- **Vishing**: Voice phishing calls pretending to be legitimate authorities.
- **Clone Phishing**: Using near-identical copies of legitimate emails to deceive users.

Stay cautious, verify sources, and never share sensitive information without confirmation.



Enjoy Extended Returns Through January 10th. **See Details**

DIVE INTO

STAUD

The LA label's latest resort-ready drop (including exclusive swim!)

COOKIES & PRIVACY

We use operational cookies to improve your experience with personalized ads and content, as detailed in our Privacy Policy.

SMS Spoofing vs. Smishing

SMS Spoofing:

- A technique where attackers disguise their identity by sending text messages that appear to come from a trusted source (e.g., a bank or known contact).
- Goal: Manipulate recipients into trusting the message without realizing the sender is fake.

Smishing:

- A type of phishing attack conducted via SMS, often including malicious links or fraudulent requests for sensitive information.
- Goal: Trick users into clicking links or sharing credentials.

Notes:

- **Spoofing** fakes the sender's identity; **smishing** delivers deceptive content to exploit the user.
- A single message could use both techniques!

YouTube
How to Video

Fake Chat Generators

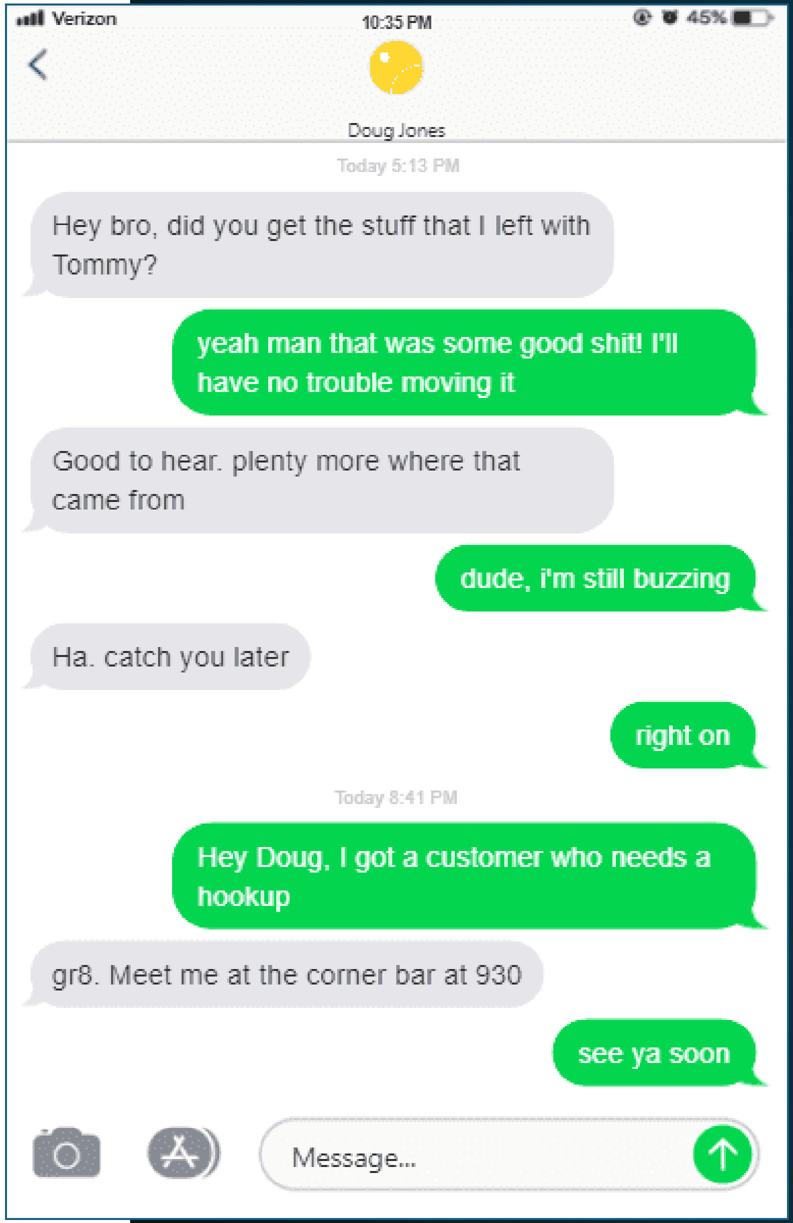
Tools that simulate realistic conversations, often imitating trusted individuals or organizations.

Security Risks:

- **Social Engineering**: Trick victims into sharing sensitive information.
- **Reputation Damage**: Spread false messages to harm credibility.
- **Financial Fraud**: Fake chats used to steal money or payment details.
- **Phishing Amplification**: Make scams seem legitimate with fabricated endorsements.

How to Mitigate:

- Verify messages through known channels.
- Raise awareness about fake chat tools.
- Use apps with message verification features.



Today 5:13 PM

Hey bro, did you get the stuff that I left with Tommy?

yeah man that was some good shit! I'll have no trouble moving it

Good to hear. plenty more where that came from

dude, i'm still buzzing

Ha. catch you later

right on

Today 8:41 PM

Hey Doug, I got a customer who needs a hookup

gr8. Meet me at the corner bar at 930

see ya soon

Fake Portrait Photo Generators

Security Risks:

- **Impersonation**: Used to create fake profiles for scams.
- **Social Engineering**: Builds trust by posing as trusted individuals.
- **Deepfake Amplification**: Complements deepfake videos for misinformation.
- **Bypassing Verification**: Tricks photo-based identity systems.
- **Eroding Trust**: Undermines confidence in digital identities.

Mitigation:

- Educate users about fake image risks.
- Use reverse image search to spot duplicates.
- Leverage AI tools to detect fake photos.

Romance Scams

A scam where fraudsters exploit emotional connections to gain money or sensitive information.

Stages of the Scam:

1. **Initial Contact**: Fake profiles on dating apps or social media.
2. **Building Trust**: Emotional conversations to deepen connections.
3. **Manipulation**: Fabricated emergencies (e.g., medical or financial troubles).
4. **Escalation**: Repeated requests for money or help.
5. **Disappearance**: Scammer vanishes once suspicions arise.

Protect Yourself:

- Verify identities; avoid sending money.
- Use reverse image searches.
- Report suspicious behavior.

Sextortion Scams

A form of blackmail where scammers threaten to release sensitive or explicit images, videos, or information unless the victim pays money or provides more compromising material.

Stages of the Scam:

1. **Initial Contact**: Scammers pose as attractive individuals on social media or dating apps to build trust.
2. **Gaining Material**: Manipulate victims into sharing explicit content or hack devices to obtain private images.
3. **Threats and Demands**: Blackmail victims with threats to share material unless paid via untraceable methods.
4. **Escalation**: Scammers may increase demands or release material despite compliance.

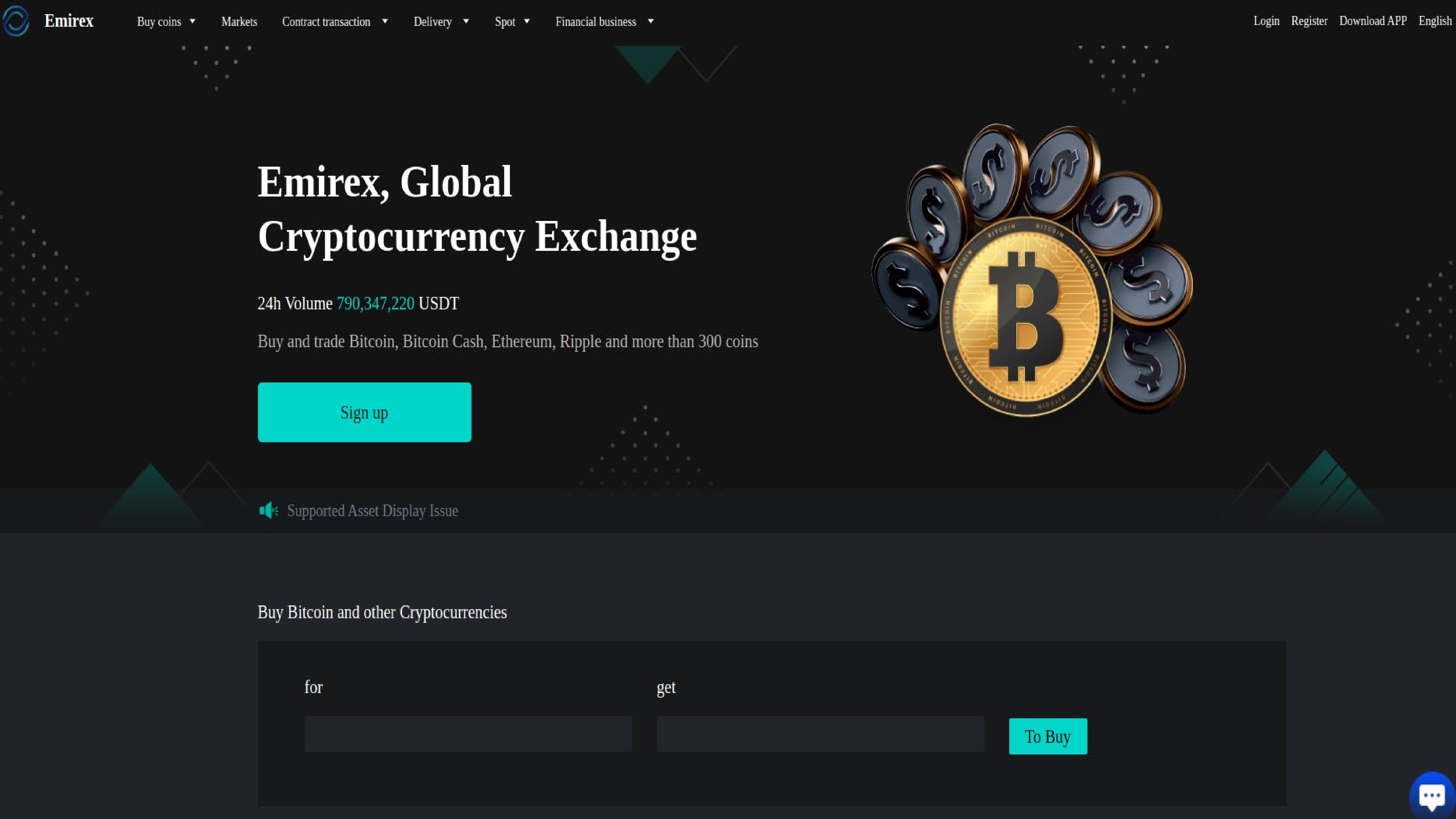
90% of the victims are boys between the ages of 14 and 17.

The Pig Butchering Scam

A scam where victims are "fattened" with trust and affection before being defrauded financially.

Stages of the Scam:

1. **Initial Contact**: Scammer poses as wealthy and successful online.
2. **Building Trust**: Develops a personal relationship over weeks or months.
3. **The Hook**: Introduces fake investment opportunities (e.g., cryptocurrency).
4. **Fattening Phase**: Victim sees fake profits and invests more.
5. **The Slaughter**: Scammer vanishes, leaving the victim with losses.



Emirex, Global Cryptocurrency Exchange

24h Volume 790,347,220 USDT

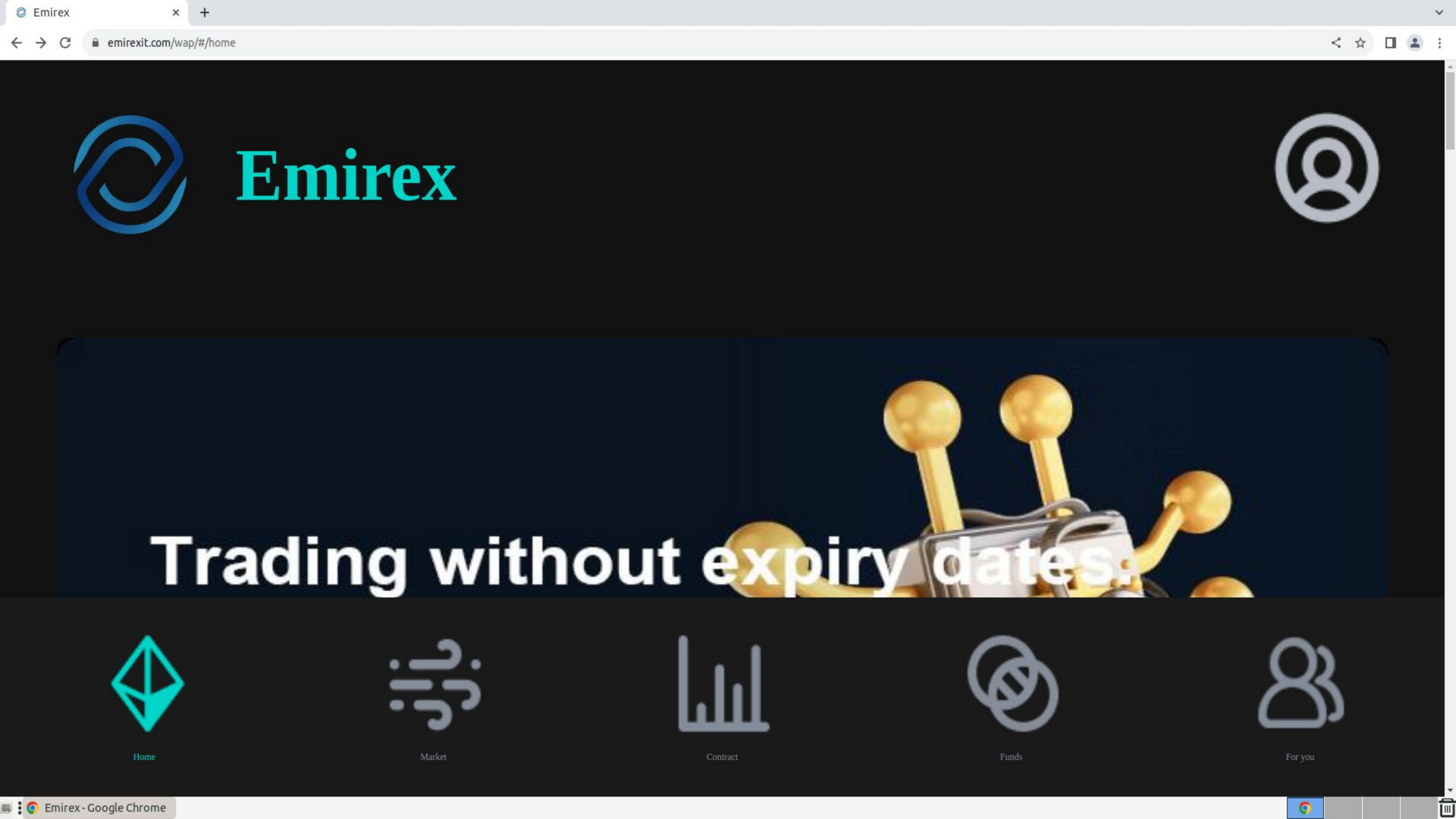
Buy and trade Bitcoin, Bitcoin Cash, Ethereum, Ripple and more than 300 coins

Supported Asset Display Issue

Buy Bitcoin and other Cryptocurrencies

for

get



Emirex

Trading without expiry dates.

The Threat of Deepfakes

AI-generated media (images, videos, audio) that convincingly mimic real people or events.

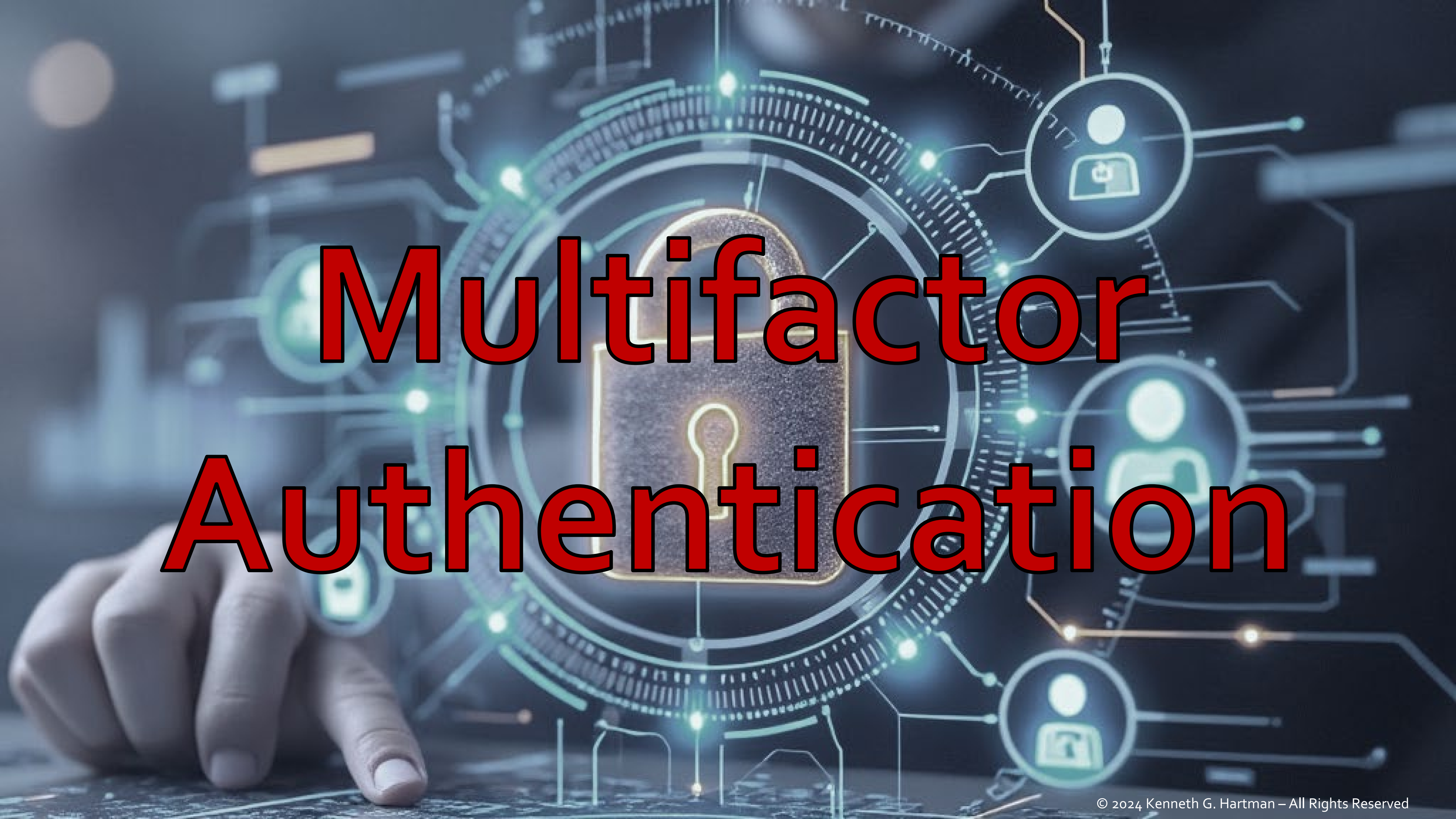
Threats:

- **Misinformation**: Spreading fake news or false narratives.
- **Identity Theft**: Impersonating individuals for fraud or bypassing security.
- **Blackmail**: Creating fake explicit content to extort victims.
- **Political Manipulation**: Fabricating videos to influence public opinion.
- **Eroding Trust**: Blurring the line between reality and fabrication.

The “deep doubt” era is here

Finance worker pays out $25 million after video call with deepfake ‘chief financial officer’

Multifactor Authentication



Multifactor Authentication

MFA is a security method requiring two or more verification factors to confirm a user's identity, adding layers of protection.

The Four Authentication Factors

1. **Something You Know**: Passwords, PINs, or security questions.
2. **Something You Have**: Devices like hardware tokens or smartphones.
3. **Something You Are**: Biometrics such as fingerprints or facial recognition.
4. **Somewhere You Are**: Location-based verification via IP address or GPS.

MFA reduces the risk of unauthorized access by requiring multiple layers of authentication.

Common MFA Methods

1. **SMS/Email Codes**: One-time passcodes sent to your device or email.
2. **Authenticator Apps**: Time-sensitive codes generated by apps like Google Authenticator.
3. **Push Notifications**: Approve or deny login attempts via a smartphone app.
4. **Hardware Tokens**: Physical devices like YubiKeys or smart cards.
5. **Biometrics**: Fingerprint, facial recognition, or voice verification.
6. **Location Verification**: Confirms login based on GPS or IP address.

How Attackers Exploit MFA Limitations

1. **Exploiting SMS MFA**:
   - **SIM-Swapping**: Hijack phone numbers to intercept codes.
   - **Interception**: Exploit vulnerabilities to steal SMS messages.

2. **Bypassing Push Notifications**:
   - **MFA Fatigue**: Spam login requests until approved.
   - **Social Engineering**: Trick victims into approving access.

3. **Phishing for MFA Codes**:
   - **Man-in-the-Middle**: Fake login pages capture codes in real time.
   - **Credential Harvesting**: Scammers request codes via phishing emails or calls.

4. **Exploiting Biometrics**:
   - **Deepfakes**: Use replicas to bypass scans.
   - **Irreversible Breaches**: Stolen biometric data cannot be reset.

5. **Circumventing Location MFA**:
   - **VPNs/GPS Spoofing**: Mask real location to bypass geographic restrictions.

There are no "perfect" security controls

How Kevin Mitnick Exploited MFA via Social Engineering

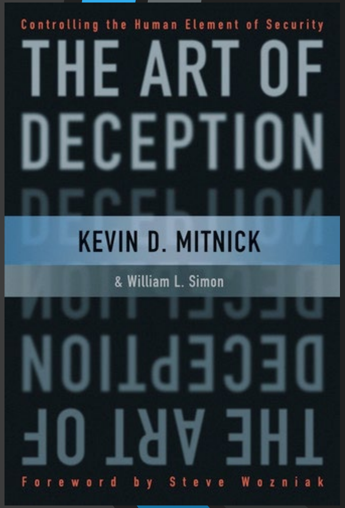
The Scenario:

- Mitnick impersonated a VP working remotely on an urgent sales presentation.
- Claimed to be locked out of his account and needed immediate help.

The Tactics:

- **Urgency**: Pressured the help desk with a tight deadline.
- **Credibility**: Used insider knowledge to sound authentic.
- **The Ask**: Requested the MFA code, claiming technical issues.

Result: The help desk provided the code, granting unauthorized access.



Controlling the Human Element of Security

THE ART OF DECEPTION

KEVIN D. MITNICK

& William L. Simon

Foreword by Steve Wozniak

SIM Swapping Attack

Social Engineering:

The attacker impersonates the victim to convince the mobile carrier to transfer their number to a new SIM.

Porting the Number:

The victim’s phone loses service, and the attacker gains control of their phone number.

Exploiting Access:

The attacker intercepts calls, messages, and SMS-based 2FA codes to take over accounts (e.g., banking, email, or cryptocurrency).

Signs You're a Victim of a SIM Swap

Can't Make Calls or Send Texts:

- Errors when texting or calling may indicate your SIM is deactivated and fraudsters are using your number.

Notifications of Activity Elsewhere:

- Alerts from your carrier about SIM activation on another device are a key warning sign.

Lost Access to Accounts:

- Login credentials no longer work, likely due to scammers changing passwords after taking over your number.

Unauthorized Transactions:

- Unexpected charges on your accounts may indicate criminals are using your credentials.

How to Protect Against SIM Swap Scams

- **Be Wary of Phishing**: Avoid clicking links in unsolicited emails or sharing personal data.
- **Strengthen Account Security**: Use strong passwords and security questions.
- **Set a Carrier PIN**: Add an extra layer of protection with a separate passcode.
- **Avoid SMS-Based Authentication**: Use authenticator apps tied to your physical device.
- **Enable Alerts**: Request activity notifications from your bank and carrier.
- **Encourage Call-Backs**: Advocate for organizations to verify identities with customer call-backs.

Google Authenticator

Secure
All your accounts
9:30
Authenticator
Search
Binance • myemail@gmail.com
29
554 450
ByBit • myemail@gmail.com
29
124 313
Gitlab • myemail@gmail.com
03
889 123
Google • myemail@gmail.com
29
914 515

Google Authenticator Cloud Backup

Introduced in April 2023, allows time-based one-time passwords (TOTPs) to sync across devices.

Benefits:

1. **Convenience**: Seamless device transitions.
2. **Reduced Lockout Risk**: Prevents loss of 2FA codes.
3. **Improved Access**: Sync 2FA codes across multiple devices.

Security Implications:

1. **Lack of E2EE**: Google holds encryption keys.
2. **Risk of Breach**: Unencrypted backups are vulnerable to exposure.
3. **Unauthorized Access**: Compromised accounts can expose all 2FA codes.

Disable Cloud Backup:
- Use local storage for 2FA codes.
- Make a local backup

Password Managers (Like 1Password)

Securely store and manage passwords and sensitive information using encryption.

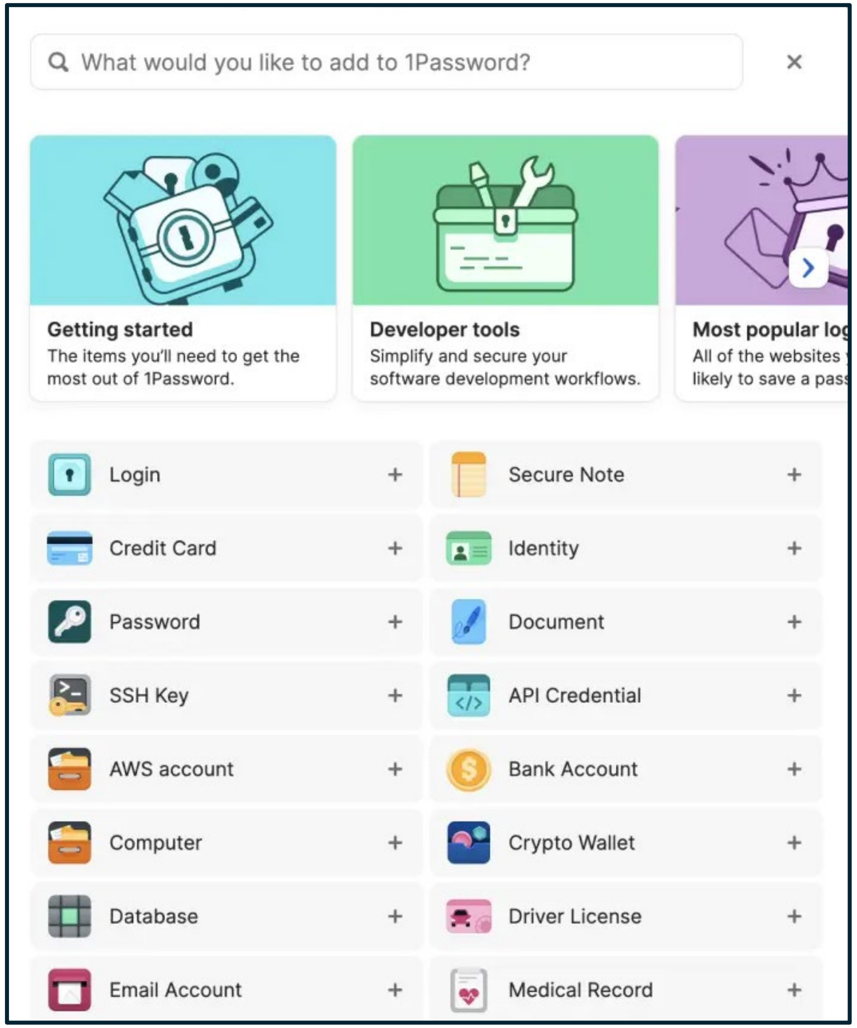
Benefits:

- **Enhanced Security**: Strong encryption and password generation.
- **Convenience**: Autofill and cross-device syncing.
- **Organization**: Store credentials, credit cards, and notes in one place.

Risks:

- **Single Point of Failure**: Compromise of the master password can expose all stored credentials.
- **Cloud Storage Risks**: Vulnerable to breaches despite encryption.
- **Cost**: Subscription fees may deter some users.

Key Takeaway: Password managers improve security and convenience but require strong master passwords and cautious usage.



What would you like to add to 1Password?

Getting started
The items you'll need to get the most out of 1Password.

Developer tools
Simplify and secure your software development workflows.

Most popular log
All of the websites
likely to save a pass

Storing Bitcoin Wallet Passwords in 1Password: Why It’s Risky

“Just Because You Can, Doesn’t Mean You Should”

- While 1Password offers strong encryption and convenience, storing Bitcoin wallet credentials introduces unnecessary risks.
- Cryptocurrency transactions are **irreversible**—a single compromise of your 1Password account could lead to permanent loss of funds.

High-Value Credentials and Blast Radius

- **High-value credentials**, such as Bitcoin private keys, should not be stored in a password manager.
- Keeping them separate reduces the **blast radius** of a potential breach—an attacker compromising your password manager won't gain access to your crypto assets.

Key Takeaway: For critical assets like Bitcoin wallets, prioritize **offline storage** and diversify where sensitive credentials are stored to limit potential damage.

What Are Passkeys?

A passwordless authentication method using cryptographic keys.

How They Work:

- **Public Key**: Stored by the website or service.
- **Private Key**: Stored securely on your device.
- **Authentication**: Device-specific actions (e.g., fingerprint, PIN) verify your identity.

Benefits:

- Resistant to phishing and brute-force attacks.
- Simplifies logins—no need to remember passwords.
- Cross-platform support with encryption for syncing.

Passkey Security and Limitations

Security Advantages:

- End-to-End Encrypted (E2EE) synchronization across devices.
- Private keys never leave your device unencrypted.
- Immune to phishing and server breaches.

Potential Limitations:

- **Cloud Backup Risks**: Encrypted passkeys could be targeted in rare cloud breaches. (Unlikely but theoretically possible.)
  - However, the attacker would also need the user's decryption keys to access the private keys.
- **Device Compromise**: If an unlocked device is stolen, passkeys could be misused.

Data Destruction

Deleting Data vs. Securely Wiping It

Deleting Data: Removes file references but leaves data recoverable. Specialized tools can retrieve it.

Securely Wiping: Overwrites data with random patterns, preventing recovery.

Tools: Use DBAN, native OS utilities, or encryption tools to securely wipe sensitive data.

Key Takeaway: Deleting is not enough for sensitive files—securely wipe to protect your data.

Synching Data Across Devices

Incomplete Deletion: Files deleted on one device may remain in the cloud or on other synced devices.

Version History: Cloud services may store older versions of files even after deletion.

Increased Exposure: Synced data is accessible across multiple devices, expanding the attack surface.

Key Takeaway: Ensure synced data is deleted everywhere and monitor cloud settings.

Handling Old Hard Drives and Cell Phones

PC Hard Drives: Securely wipe with DBAN or physically destroy (e.g., drill holes).

Cell Phones:

- Perform a factory reset and enable encryption before resetting.
- Remove SIM and SD cards.

Key Takeaway: Treat old devices as security risks—wipe or destroy them to ensure safety.

Conclusion

Building Trust in an AI-Driven World

Trust: Our greatest asset and vulnerability

Empowerment: Knowledge and tools for self-protection

Adaptation: Staying vigilant against evolving threats

Ethics: Fostering awareness and accountability

LUCID TRUTH
TECHNOLOGIES
LucidTruthTechnologies.com

Thank You!

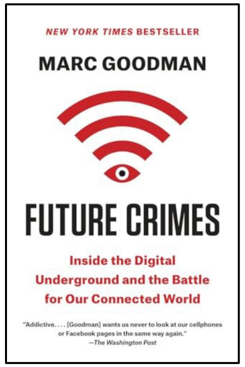
Technology evolves, but trust remains timeless.

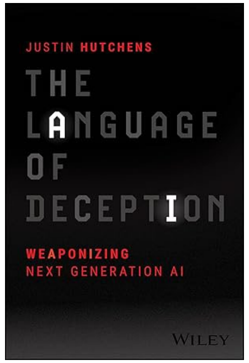
Together, we can create a more resilient and secure digital world.

Questions? Let’s continue the conversation.

Get these Slides!

bit.ly/4itTRIJ


NEW YORK TIMES BESTSELLER
MARC GOODMAN
FUTURE CRIMES
Inside the Digital Underground and the Battle for Our Connected World
"Addictive. . . . [Goodman] wants us never to look at our cellphones or Facebook pages in the same way again."
—The Washington Post



My contact info:
Ken@Lucid-Truth.com`
X: @kennethghartman
www.linkedin.com/in/kennethghartman