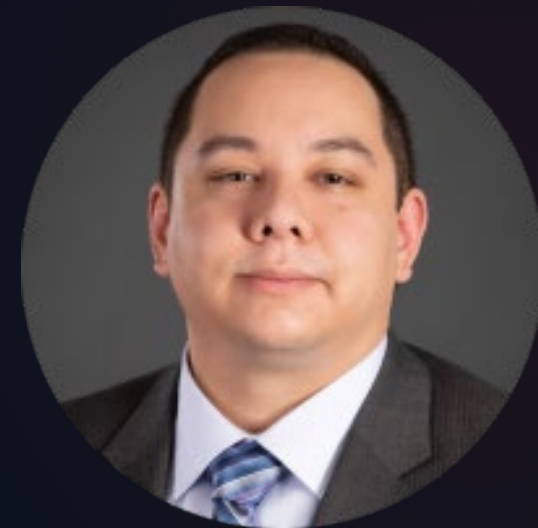


CISSP FRAMEWORK ANALYSIS

The Anatomy of Modern Scams

About Me

Mark Repka – Senior Security Consultant





ISC²: International Information System Security Certification Consortium

CISSP: Certified Information Systems Security Professional

Security and Risk Management

Asset Security

Security Architecture and Engineering

Communication and Network Security

Identity and Access Management

Security Assessment and Testing

Security Operations

Software Development Security



01 / The Scale of The Problem

| The Massive Financial Toll

\$20B+

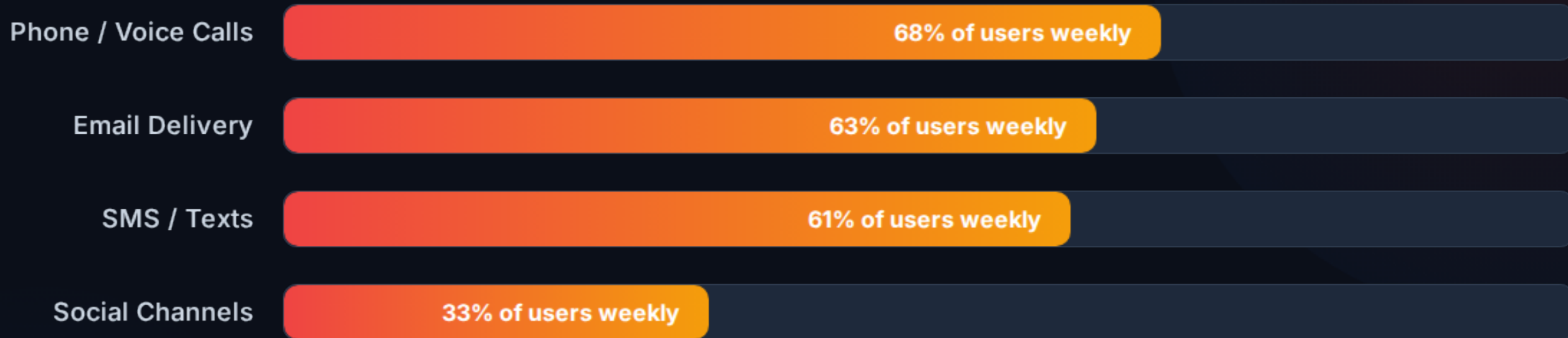
Annual Cybercrime & Scam Losses

Aggressive Modern Fraud Growth

Scammers rely on automated, multi-channel attacks targeting user trust.

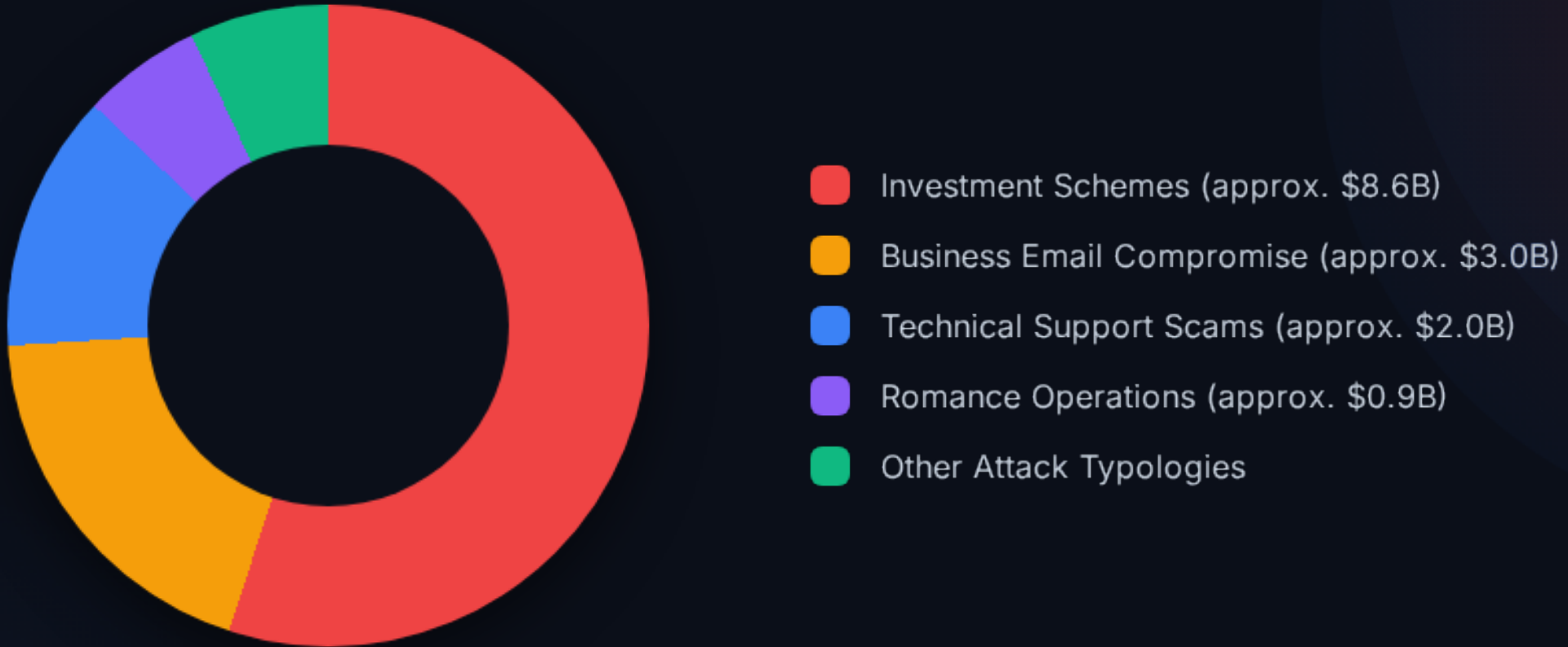
Massive data leaks provide highly localized targeting credentials, creates social engineering attacks.

Global Scam Encounter Rates



Reference Stats: Pew Research. High weekly exposure rates across multiple channels highlight that technology protections must be paired with continuous social engineering awareness training.

Distribution of Cybercrime Damages



Financial data metrics derived from FBI IC3. Although email attacks represent slightly lower volumes, targeted wire transfers and high-urgency invoice schemes lead to high financial losses.

Beyond the Dollar – Non-Financial Motivations

Why Scammers Target You (It's Not Just About Cash)

Data Collection & Harvesting:

Personal identifiers

Account Takeover & Impersonation:

Hijacking email, messaging, or social

Theft of Sensitive Information:

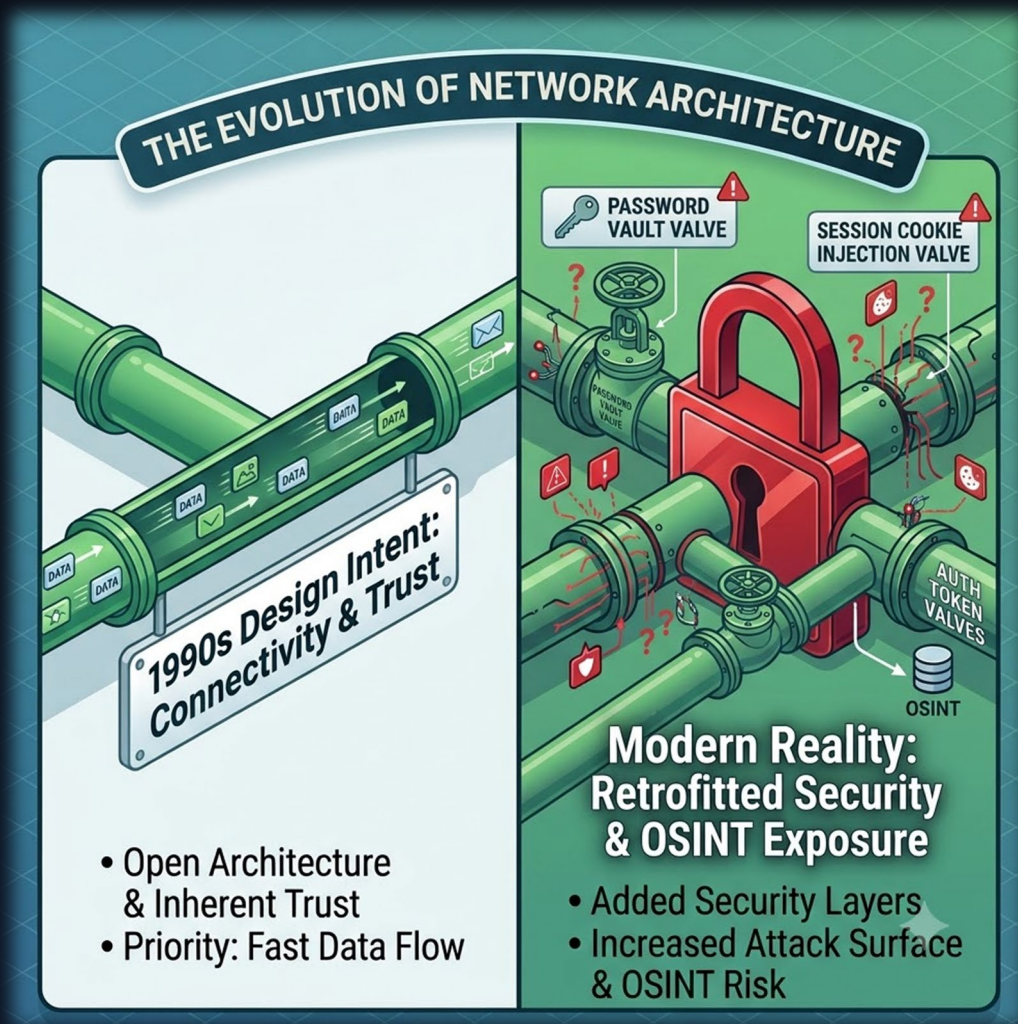
Intellectual property, login credentials

MFA Bypass & Credential Stashing:

Security Bypassing



Root Cause – Open Connectivity vs. Built-In Security



Design Legacy of the Web & Social Platforms

Architecture Built for Trust

Social Media Footprinting

Structural Vulnerability



02 / CISSP Human Vector Standards

CISSP Influence Principles



Authority

Exploits
organizational
hierarchy



Time Sensitivity

Creates
artificial
urgency



Exclusivity

Leverages
scarcity



Helpfulness

Exploits
liking and
social
consensus



Manipulation Tactic – Authority

Executive & Regulatory Impersonation

Definition: Scammers exploit high-status positions, organizational hierarchies, or regulatory power to enforce immediate compliance without questioning.

Psychological Mechanism: People are socially conditioned to respect authority figures and defer judgment to management, legal entities, or technical experts.

Examples:

CEO/Executive Wire Request

IT Helpdesk Account Audit

Government/Regulatory Fine



Manipulation Tactic – Time Sensitivity



Artificial Urgency & Fear of Loss

Definition: Threat actors construct short, artificial deadlines to induce panic and force rapid action.

Psychological Mechanism: High stress and limited response windows overload cognitive processing, causing victims to bypass critical reasoning and standard verification protocols.

Examples:

Imminent Account Termination

Urgent Fraud Alert Call

Expired Delivery Notice



Manipulation Tactic – Exclusivity

Scarcity & Selective Targeting

Definition: Attackers convince victims that they have been selected for a rare, limited-time opportunity or exclusive remedy.

Psychological Mechanism: Exploits the Fear Of Missing Out (FOMO) and the human tendency to place higher value on information or offers perceived as restricted or elite.

Examples:

VIP Investment Portals

Executive Beta Testing/Modifications

Restricted Tax/Grant Settlement





Manipulation Tactic – Helpfulness

Exploiting Support & Good Faith

Definition: Scammers pose as friendly, helpful assistants or present a customer service issue that appeals to the victim's desire to solve problems.

Psychological Mechanism: Leverages the social principle of reciprocity and natural helpfulness—when someone appears to be assisting you, you naturally lower your guard and trust them.

Examples:

Fake Vendor Customer Support
Friendly IT Onboarding Assistant
Accidental Transfer Refund

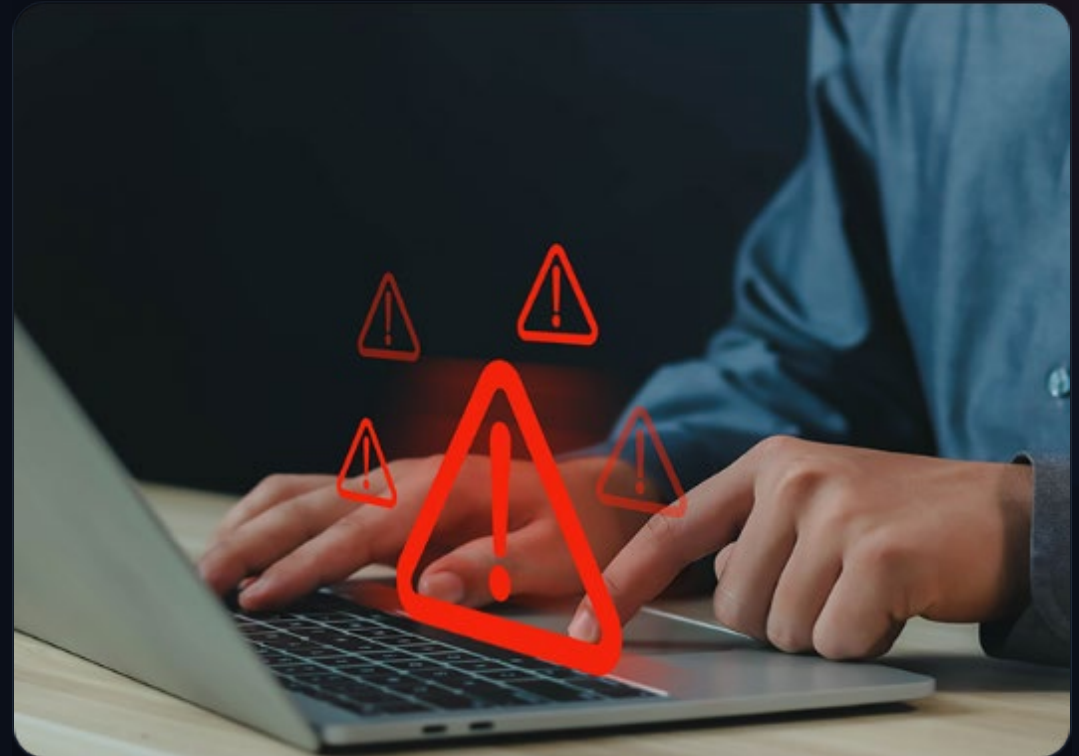


| Targeted Email & Phishing Tactics

Technical and Visual Hijacking

Phishing campaigns manipulate basic user interfaces to hide highly malicious intents:

- ⚠ **Business Email Compromise (BEC)**
- ⚠ **Spear Phishing & Whaling**
- ⚠ **Technical Exploits**



| Business Phishing Blueprint

Business Email Compromise

Highly targeted exploits mimicking senior executives or external vendors. They leverage **Authority** and **Urgency** to demand fraudulent wire transfers or bypass invoice reviews.

Spear Phishing & Whaling

Spear phishing uses tailored context derived from open-source intelligence. Whaling specifically aims at C-suite leaders with high-level access, exploiting **Exclusivity** and trusted channels.

| SMS Smishing Exploits High-Response Mobile Vectors

Definition: Smishing is a form of phishing that uses fraudulent text messages (SMS)

SMS Smishing Mechanics



Vishing: Real-Time Phone Coercion

Definition: Vishing (voice phishing) is a form of social engineering where attackers use phone calls or voice messages.

Voice phishing (Vishing) leans heavily on dynamic verbal manipulation

⚠️ **Caller ID Masquerading**

⚠️ **Exploiting Intimidation**

⚠️ **System Compromise**

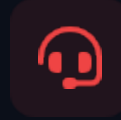


| The Next Wave: AI Generative Scams



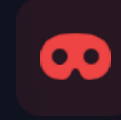
Voice Synthesizers

Using 3-second public audio samples to generate voice clones that impersonate family members requesting emergency information or funds.



Autonomous AI Agents

Mass-scale conversational agents capable of sending customized texts or emails, scaling complex relationships and trust-building processes.



Live Deepfake Streams

Simulating executive appearances and live feeds during joint video conferencing calls, completely redefining organizational authority.



03 / Defense Strategies

| The Four Stages of an Attack Lifecycle

02 / The Hook

Attacking using the CISSP social engineering vectors to establish authority or urgency.

04 / Exfiltration

Funds are instantly transferred through multi-step mule structures or cryptocurrency pools.

01 / Footprint

Scammers compile targets via open source utilities, public profiles, and dark web leaks.

03 / Exploitation

Victims bypass corporate protocols, handing over OTP codes/information or wire authorization.

CISSP Defense Strategy

Three administrative and technical controls to secure operations:



Out-of-Band
Verification

Never reply
through the
incoming
channel



Enforce Dual-
Authorization

Separate
authorized
sources



Behavioral
Phishing Drills

Implement
context-rich
simulations

| Zero Trust Communication — Voice & Social Engineering

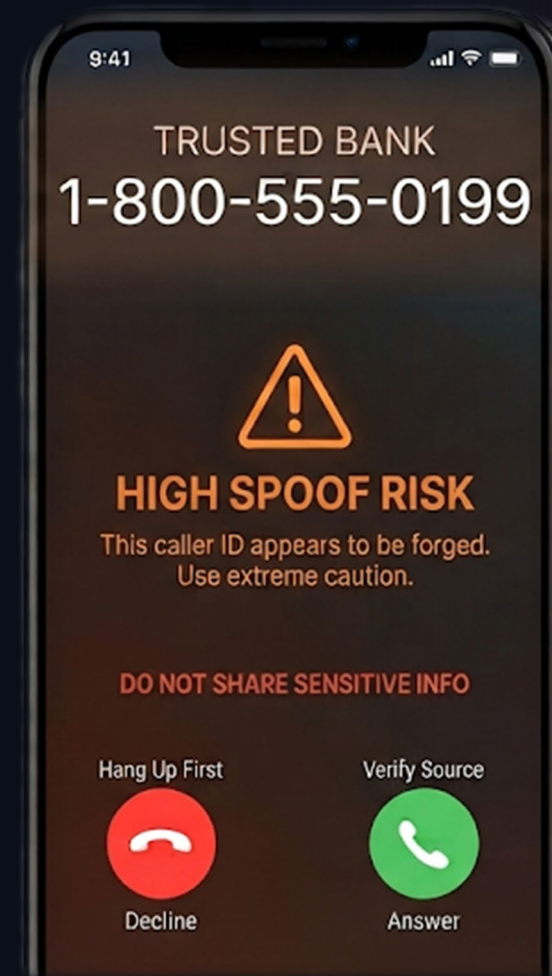
Verifying Mobile & Voice Interactions

Verify Caller Identity Independently

Refuse Immediate Action

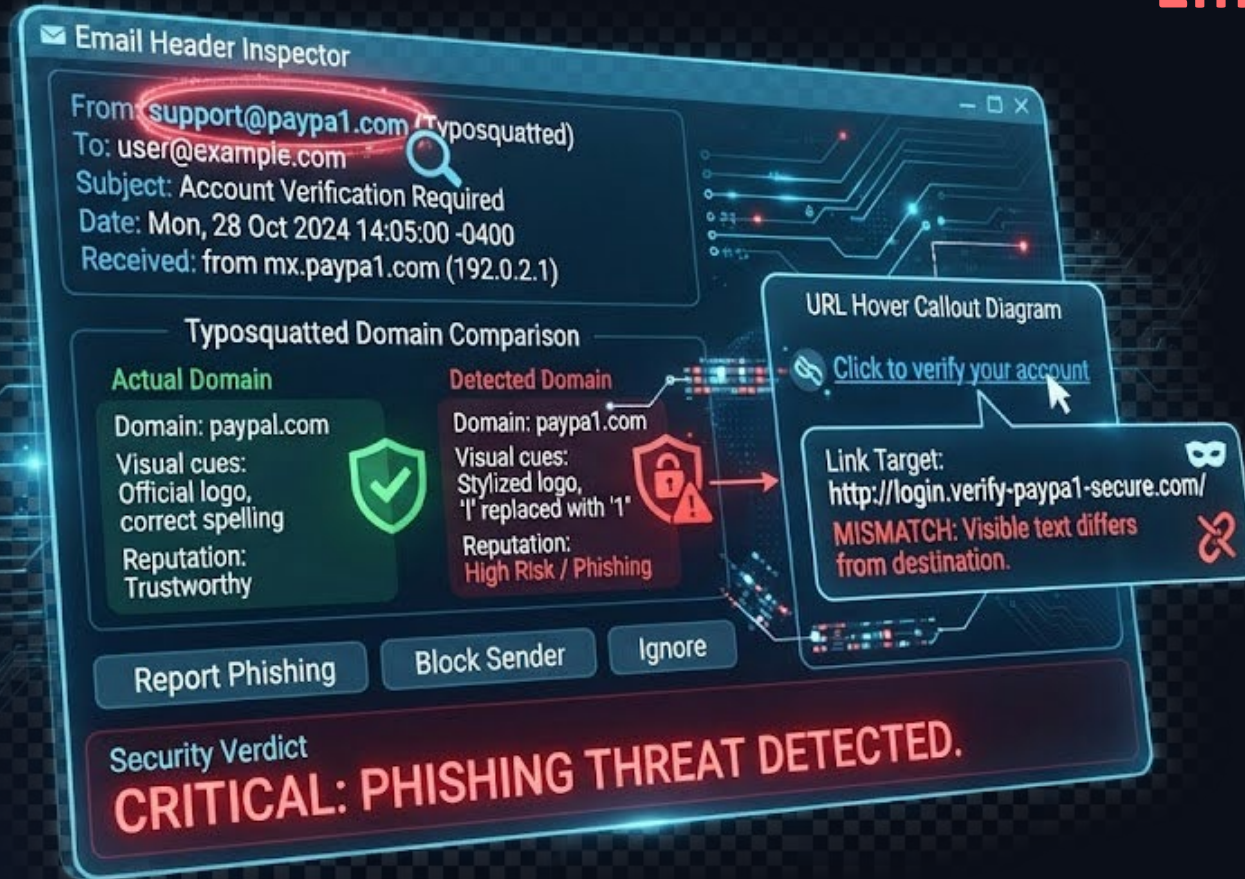
Hang Up and Call Back

Keep Sensitive Data Private



Web & Email Hygiene — Links and Headers

Email Header Parsing & Safe Browsing



Inspect the Actual Address

Avoid Direct Link Clicking

Navigate Manually

Treat Unexpected Attachments
as Hostile

Technical Hardening — Updates & System Exploits

Operating System & Application Baselines

Unpatched Kernel Vulnerabilities

Automated System Patching

Browser & Reader Exploit Vectors

Third-Party Patch Management

Environment Defensive Baseline



| Digital Footprints — Don't Feed the Bots

Continuous Data Harvesting & Weaponization

Every Click Leaves a Trace

Algorithmic Profiling

What Data Is Being Gathered?

Re: Your Privacy



Targeted Exploitation

High-Yield Social Engineering

| The Operational Rule — Doubt Everything



Adopting a Zero Trust Mindset

Adopt a Zero Trust Posture

Identify Psychological Triggers

Pause Before Acting

Validate Out-of-Band

| Navigating the Digital World with Confidence

Empowerment Through Verification

Awareness Over Anxiety

Verification is Empowerment

Build Strong Habits

Confident Connectivity





04 / Questions