Anatomy Of Phishing Attack

Cyber Security Awareness

Stay Safe Online and Secure Our World

Presenter

Tanmay Bhattacharjee a.k.a Blackhawk

Product Security Engineer at R360 Groups

Offensive and Defensive Security

Linkedin: https://www.linkedin.com/in/tanmaybhattacharjee

X : https://x.com/blackk_hawkkk

Key Points Covered

01

Understanding Phishing

02

Anatomy of Phishing Attack

03

Real world attack scenario and Example

04

Live Demonstration and safe Environment

05

Comprehensive Protection Strategy

Key Points Covered

06

Incident Response and Best Practices

Q&A

07

The Phishing Threat Landscape

83%

of organizations experienced phishing attacks in 2024
Source: Proofpoint State of the Phish 2024

$4.9M

Average cost of a data breach from phishing
Source: IBM Cost of a Data Breach Report 2024

90%

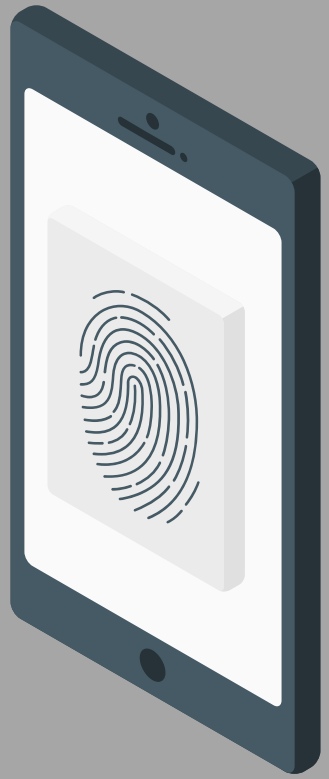
of successful cyber attacks start with phishing
Source: Verizon Data Breach Investigations Report 2024

1 in 4

people fall for phishing attempts
Source: KnowBe4 Phishing by Industry Report 2024

What is Phishing?

Phishing is a social engineering attack vector where cybercriminals impersonate trusted entities through digital communications to steal sensitive information such as credentials, financial data, or personally identifiable information (PII).



Deception

Attackers create fraudulent communications mimicking legitimate sources

Trust Exploitation

They impersonate trusted entities like banks, employers and etc

Information Harvesting

Victims are manipulated into divulging sensitive data or credentials

Types of Phishing Attacks

Email Phishing

Mass emails sent to thousands targeting general information

Spear Phishing

Targeted attacks on specific individuals or organizations

Whaling

High-value targets like CEOs and executives

Types of Phishing Attacks

Smishing

Phishing via SMS text messages

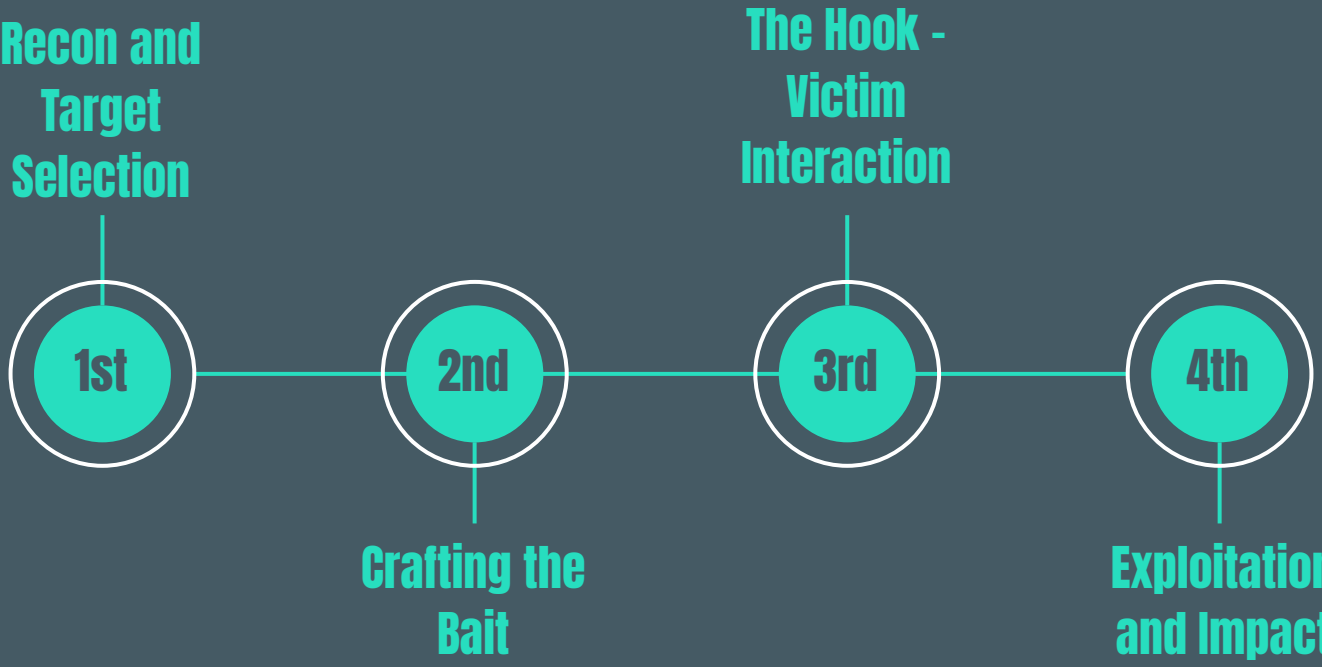
Vishing

Voice phishing through phone calls

Pharming

Redirecting users to fake websites

Anatomy of a Phishing Attack



Step 1: Reconnaissance & Target Selection

Information Gathering

- Social media profiling
- Company websites
- Public databases
- LinkedIn profiles

Target Identification

- High-value individuals
- Vulnerable employees
- Access to sensitive systems
- Financial authority

Step 2: Crafting the Bait

Email Creation

- Spoofed sender addresses
- Company logos & branding
- Urgent language
- Official-looking templates

Psychological Triggers

- Fear & urgency
- Authority figures
- Curiosity & rewards
- Social validation

Target Identification

- High-value individuals
- Vulnerable employees
- Access to sensitive systems
- Financial authority

Step 3: The Hook – Victim Interaction

Initial Contact

- Email delivery
- SMS message
- Phone call
- Social media message

Victim Response

- Clicks malicious link
- Downloads attachment
- Provides information
- Calls fake number

Data Collection

- Login credentials
- Credit card details
- Personal information
- System access

Step 4: Exploitation and Impact

Immediate Action

Account takeover
Financial theft
Identity theft
System infiltration

Secondary Attack

Lateral movement
Data exfiltration
Ransomware deployment
Further phishing

Long Term Damage

Financial losses
Reputation damage
Legal consequences
Regulatory fines

How to spot Phishing : Red Flags

Senders Issues

Unfamiliar sender
Mismatched domains
Generic greetings

Urgency and Threat

Act immediately
Account suspended
Limited time offer

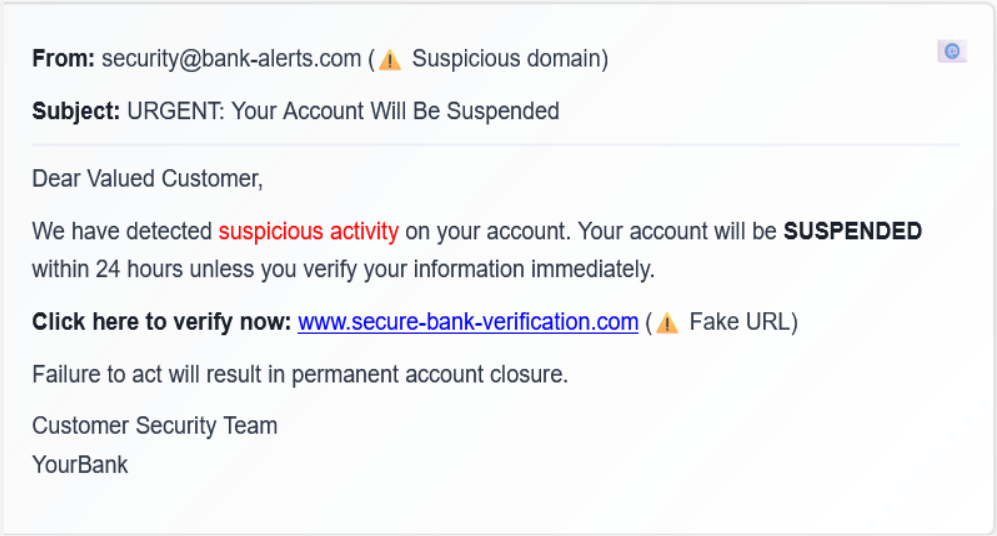
Suspicious Link

Shortened URLs
Misspelled domains
HTTP instead of HTTPS

Attachment

Unexpected files
Executable files
Compressed archives

Time of POC



Red Flags: Urgency, threats, suspicious domain, generic greeting, poor grammar

Protection Strategies

Verify Before Trust

Check sender addresses
Hover over links
Call to confirm
Visit sites directly

Technical Defenses

Use 2FA/MFA
Keep software updated
Use email filters
Install antivirus

Stay Informed

Security training
Threat intelligence
Company policies
Report incidents

Incident Response

Disconnect devices
Change passwords
Report to IT/Security
Monitor accounts

You Are the Human Firewall!

REMEMBER: TECHNOLOGY + HUMAN AWARENESS = STRONG DEFENSE

🤔 Think

Is this email/message expected? Does it make sense?

⏸️ Pause

Don't rush. Take time to analyze before acting.

✅ Verify

Confirm through alternative channels before responding.

Golden Rule: When in doubt, DON'T click, DON'T respond, and ASK for help!

MITRE ATT&CK – Phishing (T1566): Enterprise

Technique	Description	Sub-techniques
T1566 – Phishing	Adversary delivers social engineering content via email or communication channels to obtain credentials or initial access.	T1566.001 – Spearphishing Attachment Malicious files (Office, PDF, ZIP) T1566.002 – Spearphishing Link Links to credential harvesters or malware sites. T1566.003 – Spearphishing via Service Phishing via cloud/email services (Teams, Slack, Gmail, Outlook 365). M1032 – MFA (Phishing-resistant)

Phishing Mitigation Layers : Enterprise

Prevention / hardening

- Enforce MFA (M1032), especially phishing-resistant
- Application control / execution prevention (M1038)
- Restrict software installs/untrusted code (M1033, M1035)
- Keep software patched (M1051)
- Harden OS, boot integrity, code signing (M1046, M1045)

Filtering / blocking

- Network traffic filtering (M1037), intrusion prevention (M1031)
- Restrict web content, disable risky browser features (M1021)
- Use threat intelligence (M1019) to block known bad domains

Detection / isolation

- Use endpoint behavior prevention (M1040).
- Sandboxing / isolation of attachments (M1048).
- Audit / logging (though Audit is more general mitigation).
- Threat intelligence integration to detect attacks early.

Phishing Mitigation Layers : Enterprise

User-focused defenses

- Train users (M1017).
- Provide easy reporting mechanisms (so users can escalate suspicious emails).

Containment / minimizing impact

- Restrict lateral movement (M1035).
- Credential protection (M1043).
- Least privilege practices.
- Network segmentation to restrict what compromised systems can access.

Ref:

Tactics: https://attack.mitre.org/tactics/TA0001/

Technique: https://attack.mitre.org/techniques/T1566/

Defenses : https://attack.mitre.org/mitigations/enterprise/

Resources

🏛️ Government Resources

CISA Cybersecurity Tips
FBI IC3 Reporting
FTC Consumer Alerts

🎓 Training Platforms

KnowBe4 Security Training
SANS Security Awareness
Proofpoint Security

🔧 Security Tools

Email security gateways
Password managers
2FA applications

🌍 Real-World Phishing Scenarios

Business Email Compromise

CEO impersonation leading to wire fraud

Educational Institution Attack

Student credential harvesting campaign

Healthcare Data Breach

COVID-19 themed attacks on hospitals

Business Email Compromise Attack POC

From: ceo.john.smith@company-urgent.com (⚠️ Look-alike domain)

Subject: URGENT - Confidential Wire Transfer Required

Hi Sarah,

I'm currently in meetings with potential investors and need you to process an urgent wire transfer for the acquisition deal we discussed.

Amount: $150,000
Recipient: Global Investment Partners LLC
Account: [Bank details provided]

This is time-sensitive. Please process immediately and confirm.

Thanks,
John Smith
CEO

🚩 **Red Flags: Urgency, external pressure, unusual requests, slight domain misspelling**

Social Media Phishing Attack

🎯 Exciting Security Consulting Opportunity - URGENT

Hi there!

I saw your impressive cybersecurity background on LinkedIn and was truly impressed by your expertise. I work for a **major Fortune 500 technology company** and we have an **urgent security consulting opportunity** that would be perfect for someone with your skills.

⚠️ **This is highly confidential** and time-sensitive ⚠️

Can you click this link to review the project details and compensation package? **The position pays $200K+ annually** and comes with significant bonuses.

🔗 View Confidential Job Details ➡️

🚨 Malicious Link: bit.ly/urgent-consulting-offer-2025-secure-login

Please respond within the next 24 hours as we're interviewing candidates this week.

Best regards,
Sarah Johnson
Senior Technical Recruiter | TechCorp Solutions
📧 sarah.johnson@techcorp-recruitment.net

Red Flags

Flattery bombardment
Suspicious domain
Shortened URLs

Psychological Manipulation

Professional ego appeal
Career advancement desire
Social proof

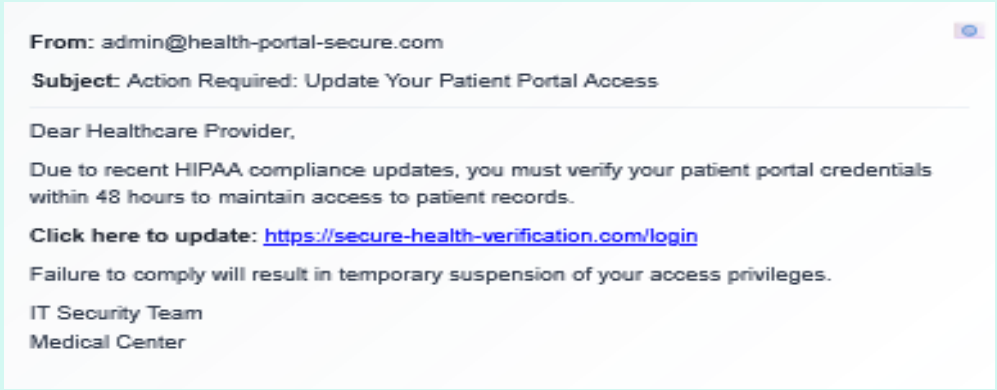
Protection Tips

Verify the sender
Research the company
Never click suspicious links

Why Social Media Phishing Works:

Trust Factor: Professional networks create inherent trust • **Career Motivation:** People want better opportunities • **Social Proof:** Connection status implies legitimacy • **Information Availability:** Profiles provide targeting data

Healthcare Sector Phishing Attack



From: admin@health-portal-secure.com

Subject: Action Required: Update Your Patient Portal Access

Dear Healthcare Provider,

Due to recent HIPAA compliance updates, you must verify your patient portal credentials within 48 hours to maintain access to patient records.

Click here to update: https://secure-health-verification.com/login

Failure to comply will result in temporary suspension of your access privileges.

IT Security Team
Medical Center

💡 **Why Healthcare is Targeted:** High-value data, time pressure, life-critical systems, stressed professionals

Mobile Phishing (Smishing) Attack

Banking SMS Scam

⚠ SUSPICIOUS MESSAGE

BANK ALERT:
Unusual activity detected on your account ending in 1234. Your account will be **LOCKED** in 2 hours.

Verify immediately: bit.ly/bank-verify-urgent

Reply STOP to cancel.

🚩 Red Flags: Urgency, shortened URL, generic account reference, threat of account closure

Package Delivery Scam

📦 FAKE DELIVERY

FedEx Delivery Update:
Package delivery to 123 Main St failed due to incorrect address.
Delivery fee required: $3.95

Reschedule & pay: fedex-redelivery.net/track?id=ABC123

Package will be returned in 24 hours.

🚩 Red Flags: Unexpected delivery fee, suspicious domain (.net instead of .com), time pressure

Credit Card Alert Scam

💳 CREDIT ALERT

Visa Security Alert:
$847.99 charge at Amazon was **DECLINED** due to suspicious activity.

If this wasn't you, secure your account now: visa-security-center.com/verify

Time sensitive - expires in 1 hour.

🚩 Red Flags: Creates false sense of security, fake domain, artificial time limit, high dollar amount

Mobile Phishing (Smishing) Attack

Mobile-Specific Vulnerabilities

1. Small screens hide suspicious URL details
2. Touch interfaces make accidental clicking easier
3. Always connected - people check messages anywhere, anytime
4. App notifications can be spoofed to look legitimate
5. Auto-preview features can execute malicious code

Mobile Phishing (Smishing) Attack

Protection Tips for Mobile:

🔍 Long-press links to preview URLs before clicking
📞 Call the company directly using official numbers
🏦 Use official apps instead of clicking text links
⏸️ Pause and think - urgency is often fake
🚫 Never provide personal info via text

Advanced Persistent Phishing

Reconnaissance Phase

Social media monitoring
Company research
Employee identification
Technology stack analysis

Trust Building

LinkedIn connections
Industry event mentions
Helpful information sharing
Professional conversations

The Hook

Personalized attack
Leveraged trust
Specific company context
Convincing pretext

Comprehensive Protection Framework

Organizational Level

Security awareness training (monthly)
Phishing simulation exercises
Email security gateways
Multi-factor authentication
Incident response procedures

Technical Controls

DMARC/SPF/DKIM implementation
URL filtering and sandboxing
Endpoint detection and response
Zero-trust network architecture

Individual Best Practices

Verify requests through separate channels
Use password managers
Enable account alerts
Regular security training
Report suspicious activities

What to Do When Phished

Immediate Actions

Disconnect from network
Don't click any more links
Take screenshots of evidence
Note time and details

Damage Assessment

Check for unauthorized access
Review recent transactions
Scan for malware
Identify compromised accounts

Recovery Actions

Change all passwords
Contact banks/credit cards
Report to IT security
File reports with authorities

Building a Security-Aware Culture

Monthly Training Topics

January: Password Security
February: Social Engineering
March: Mobile Security
April: Email Security
May: Physical Security
June: Data Protection

Simulation Exercises

Monthly phishing tests
Vishing simulations
Physical security tests
Social engineering calls
USB drop tests
Tailgating exercises

Recognition Program

Security champion awards
Phishing reporters recognition
Department competitions
Success story sharing
Continuous improvement
Feedback mechanisms

Future Threats & Emerging Trends

AI & Machine Learning

Deepfake voice calls
AI-generated phishing emails
Personalized attack automation
Real-time adaptation

New Attack Vectors

IoT device exploitation
Smart home targeting
AR/VR phishing
Cloud service abuse

Defense Evolution

AI-powered detection
Behavioral analytics
Zero-trust architecture
Continuous authentication

Real vs Fake: Microsoft Login Pages

FAKE

FAKE MICROSOFT LOGIN

https://microsft-login-secure.com/auth

MS Logo **Microsft** (Notice the typo!)

Email or phone

Password

Sign in

RED FLAGS:

- Misspelled domain name
- Non-Microsoft URL structure
- Typo in company name
- Poor form styling

✓ REAL

LEGITIMATE MICROSOFT LOGIN

https://login.microsoftonline.com/

MS Logo **Microsoft**

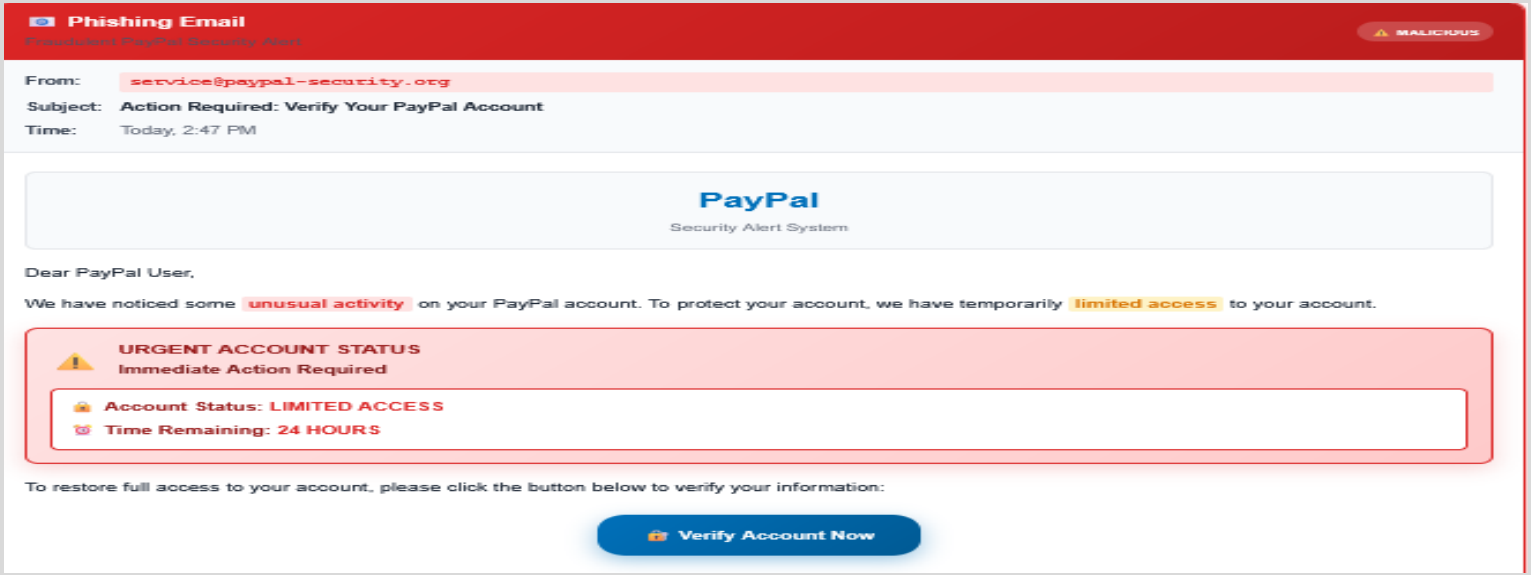
Email, phone, or Skype

Next

LEGITIMATE SIGNS:

- Official Microsoft domain
- Correct URL structure
- Professional styling
- HTTPS security

PayPal Phishing Attack Analysis



- **Red Flags**

  Use .org
  Dear PayPal User
  Creates Panic

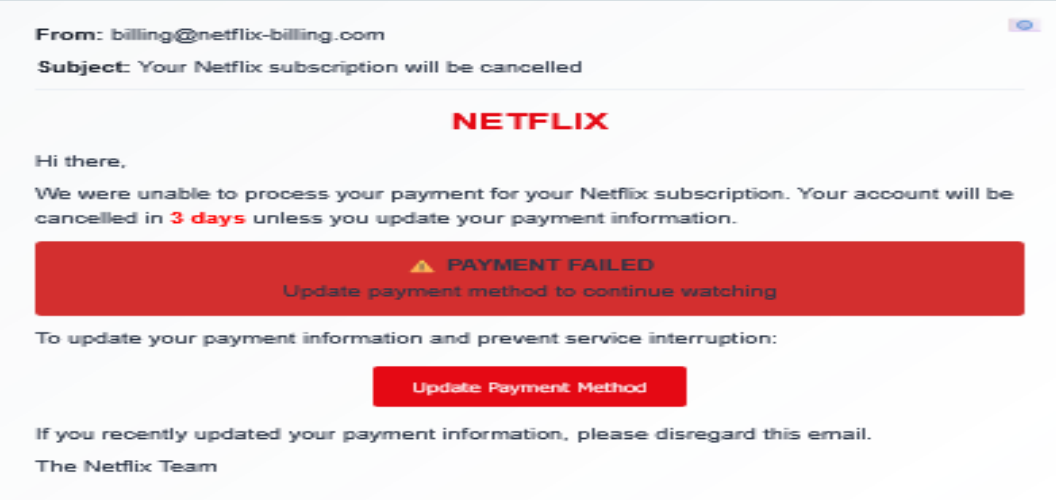
- **Psychological Manipulation**

  Permanent suspension
  Immediate Action Required
  24 hours count down

- **Verify Legitimacy**

  Go to Paypal Manually
  Real email shows your name
  Check URL destination

Netflix Subscription Scam



From: billing@netflix-billing.com

Subject: Your Netflix subscription will be cancelled

NETFLIX

Hi there,

We were unable to process your payment for your Netflix subscription. Your account will be cancelled in **3 days** unless you update your payment information.

⚠ PAYMENT FAILED
Update payment method to continue watching

To update your payment information and prevent service interruption:

Update Payment Method

If you recently updated your payment information, please disregard this email.

The Netflix Team

- **Tactics**

  Fear of Service Loss
  Time Pressure
  Familiar Branding

- **Verify Legitimacy**

  Check official Netflix domain
  Check Payment Method in account

Romance Scams & Dating App Phishing

$1.3B

Lost to romance scams in 2022

70%

of romance scam victims are women 50+

🎭 Common Personas

- Military personnel overseas
- Successful businessperson traveling
- Widowed with children
- Oil rig worker/doctor abroad

💔 Red Flags

- Professes love very quickly
- Avoids phone/video calls
- Stories don't add up
- Asks for money/gifts

💰 Common Requests

- "Emergency" medical bills
- Travel money to visit you
- Investment opportunities
- Help with customs/legal fees

🛡️ **Protection:** Never send money to someone you've only met online. Use reverse image search on profile photos. Be wary of perfect grammar from someone claiming to be from a non-English speaking country.

Advance Protection Framework

- **Zero Trust Security**

Verify every user and device
Assume breach mentality
Continuous authentication
Micro-segmentation
Least privilege access

- **AI-Powered Defense**

Behavioral analysis engines
Real-time threat detection
Automated response systems
Pattern recognition
Adaptive security policies

- **Threat Intelligence**

Global threat feeds
Industry-specific indicators
Dark web monitoring
Attack pattern analysis
Predictive threat modeling

Top 10 Phishing Attack Tools

1. Evilginx2
2. Gophish
3. Social-Engineer Toolkit (SET)
4. KingPhisher
5. HiddenEye
6. Modlishka
7. Wifiphisher
8. Zphisher
9. Phishing Frenzy
10. BlackEye

Tools

1️⃣ Email Header Analysis
Tools: MailHeader, MXToolbox, Google MessageHeader, Azure Analyzer

2️⃣ URL & IP Reputation Checks
VirusTotal, URLScan, AbuseIPDB, Talos, BrightCloud, CheckPhish

3️⃣ File & Malware Analysis
AnyRun, Cuckoo Sandbox, Hybrid Analysis, JoeSandbox, VMRay

4️⃣ Domain & WHOIS Lookups
DomainTools, SecurityTrails, DNSlytics, WHOIS

5️⃣ Automated Phishing Analysis
CyberChef, PhishTool

6️⃣ Phishing Intelligence & Blocklists
OpenPhish, PhishTank, PhishingArmy, HaveIBeenPwned

7️⃣ Learning Resources
CISA guides, SANS whitepapers, tutorials, and hands-on labs

Lab

- **TryHackMe**

  https://tryhackme.com/module/phishing

- **Range Force**

  https://www.rangeforce.com/platform

- **Gophish**

  https://getgophish.com/

Courses

- **TCM Security**

https://academy.tcm-sec.com/p/practical-phishing-campaigns

- **Hack Smarter**

https://www.hacksmarter.org/courses/3f9917b1-13b0-48f4-b43f-387e245656e7

Time of Demo

Educational Purpose

SOC FAQ

https://github.com/blackkhawkk/Anatomy_Phishing_Attack_Oct_2025/blob/main/SOC_FAQ.md

Thank You! 🙏

Stay Safe Online

LinkedIn https://www.linkedin.com/in/tanmaybhattacharjee

X : https://x.com/blackk_hawkkk

Remember the Golden Rules:

🧐 Think before you click
✅ Verify suspicious communications
🛡️ Use multi-factor authentication
📚 Keep learning about cybersecurity

Together, we can build a safer digital world! 🌎🔒