Digital Deception: Unmasking Modern Fraud Tactics and Defenses

SCAN ME

JOHN FICK, MLS, CFE, CFCI, CECFE

DIRECTOR OF FRAUD
NORTHWEST BANK

JOHN.FICK@NORTHWEST.COM
469.400.2885

VISIT NOW www.JohnFick.info

AGENDA

01 Identity Theft

02 Phishing Attacks

03 SIM SWAP

04 Injection Attacks

Key Objectives

- Understand Identity Theft: Define identity theft, recognize common methods used by fraudsters to steal personal information, identify warning signs of potential identity theft incidents and identify prevention and response strategies.

- Identify Different Types of Phishing Attacks: Explain the various types of phishing attacks, including email phishing, smishing (SMS phishing), vishing (voice phishing), and spear phishing, understand how each method is used to exploit victims, and identify prevention and response strategies.

- Recognize SIM Swap Fraud: Describe the SIM swap attack process, understand how fraudsters gain control of victims' mobile numbers, identify key red flags that indicate a potential SIM swap attempt, and identify prevention and response strategies.

- Analyze Injection Attacks: Define injection attacks such as SQL injection and code injection, understand how they exploit vulnerabilities in digital systems, and identify prevention and response strategies to mitigate these attacks.

Identity Theft

Identity Theft Defined



Identity Theft

Occurs when someone uses another person’s personal information-such as their name, Social Security Number, or credit card details to obtain money, credit, goods, or services fraudulently.

Synthetic Identity Theft

Occurs when fraudsters create a new identity by combining real and fake information often using a legitimate Social Security number (typically from a child or inactive person) with a fictitious name, date of birth and other personal details.

Identity Theft - Common Methods



- **Phishing** - Fake emails, texts, or websites that trick users into giving up personal information
- **Social Engineering** - Manipulating people into revealing confidential data (e.g., pretending to be IT Support
- **Skimming** - Hidden devices placed on ATMs or point of sale systems to steal card data
- **Data Breaches** - Hacking into organizations to access large volumes of personal information

- **Dumpster Diving** - Retrieving discarded documents that contain sensitive data
- **Public Wi-Fi Snooping** - Intercepting data over unsecured public networks
- **Malware & Spyware** - Installed via email attachments or downloads to steal data silently
- **Shoulder Surfing** - Observing someone entering a PIN or password in Public





Identity Theft Impact

Personal Impact

- **Financial Loss** - Unauthorized charges, drained accounts, stolen tax refunds
- **Credit Damage** - Lower credit scores, denied loans or housing
- **Emotional Stress** - Anxiety, frustration, and a long recovery process
- **Time & Cost to Recover** - Hours spent dealing with banks, credit bureaus, and law enforcement



Organizational & Societal Impact

- **Increased Fraud Costs** - Banks, insurers, and businesses absorb major losses
- **Loss of Trust** - Damaged reputation by organizations involved in breaches
- **Law Enforcement Burden** - Growing caseloads for digital crime and fraud investigators
- **National Security Risks** - In some cases, identity theft supports larger criminal networks

Identity Theft AI Impact

How does AI Enable Identity Theft

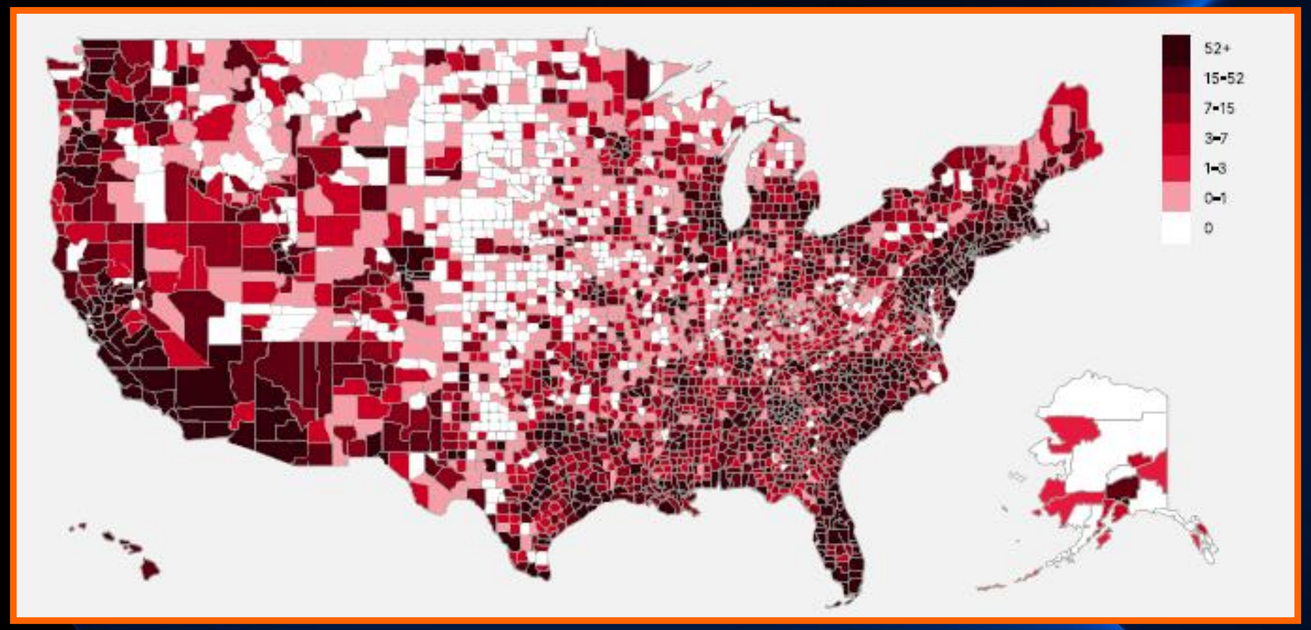
- **Deepfakes & Voice Cloning** - Fraudsters use AI to mimic voices or faces to bypass security or trick victims
- **AI-Powered Phishing Attacks** - AI can craft highly personalized and convincing phishing emails or texts
- **Data Mining & Reconnaissance** - AI can analyze massive amounts of leaked or public data to build synthetic identities or target individuals more effectively
- **Password Cracking** - AL accelerates brute force and pattern recognition to break into accounts
- **Chatbot Impersonation** - AI bots can convincingly pose as a customer service agents to extract sensitive information



How AI Helps Prevent Identity Theft

- **Anomaly Detection** - AI systems detect unusual spending patterns, login behavior, or device changes
- **Facial Recognition & Biometrics** - Enhances identity verification and account access controls
- **Natural Language Processing (NLP)** - Identifies phishing attempts in emails or texts by analyzing language patterns
- **Real-Time Fraud Alerts** - AI-driven systems can instantly flag suspicious transactions for review or automatic blocking

Identity Theft Statistics



Above is a heatmap illustrating the raw number of synthetic fraud applications for the second half of 2024. This looks very similar to the population heatmap of the United States. *SentiLink Fraud Report 2024

2024

$47 Billion Stolen

AMERICAN ADULTS LOST $47 BILLION TO IDENTITY FRAUD AND SCAMS IN 2024, AN INCREASE OF $4 BILLION OVER 2023, ACCORDING TO AARP COSPONSORED REPORT

Identity Theft Potential Warning Signs



Unfamiliar Charges or Withdrawals



Bills or Statements Stop Arriving



Unauthorized New Accounts or Credit Inquires



Debt Collectors Calling for Unknown Debts



Denied Credit Despite Good History



Login Attempt Notifications from Unknown Devices or Locations



Unusual or Perfectly Personalized Phishing Emails



Unexpected Two-Factor Authentication Alerts

Identity Theft Prevention Strategies

- **Protect Personal Information**
  - Do NOT share sensitive info over unsecured networks or with unknown contacts
  - Shred documents before discarding

- **Use Strong Passwords & Multi-Factor Authentication**
  - Create unique, complex passwords
  - Enable MFA on ALL financial and sensitive accounts

- **Monitor Accounts and Credit Reports**
  - Regularly review credit reports (at least annually)
  - sign up for transaction alerts on bank and credit accounts

- **Avoid Phishing & Social Engineering Scams**
  - Be skeptical of unsolicited calls, emails, or messages asking for information

- **Secure Devices and Networks**
  - Keep software up-to-date
  - Use antivirus and VPNs when accessing sensitive info on public Wi-Fi



Identity Theft Response Strategies

- **Report & Freeze**
  - Contact banks, credit bureaus, and freeze credit reports and ChexSystems
  - Report to the FTC at identitytheft.gov
- **File Police and IRS Reports (If Necessary)**
  - Especially for financial, medical, or tax identity theft cases
- **Notify Affected Organizations**
  - Inform employers, insurance companies, and financial institutions



- **Document Everything**
  - Keep detailed records of calls, reports and actions taken
- **Monitor for Continued Activity**
  - Stay Vigilant even after resolving the initial incident

The FTC estimates that it can take approximately 6 months and 200 hours of work to recover from an identity theft



- How much personal information do you think thief needs to successfully steal your identity?
- When was the last time you checked your credit report?

Phishing Attacks

Phishing Defined

Phishing is a type of cyberattack where a bad actor impersonates trusted sources often via email, text, or websites to trick victims into revealing sensitive information such as usernames, passwords, or financial data.

Key Points:

- Disguised as legitimate communication (e.g., from banks, coworkers, or companies
- Uses a sense of urgency or fear to prompt a quick action
- Can lead to identity theft, data breaches, or financial loss

> Over 90% of cyberattacks begin with a phishing email. Verizon Data Breach Investigations Report

Phishing Example - BEC

Business Email Compromise (BEC)

BEC is a cyber-enabled fraud where a bad actors use spoofed or compromised email accounts to deceive individuals into transferring money or sensitive data

Phishing Example - BEC



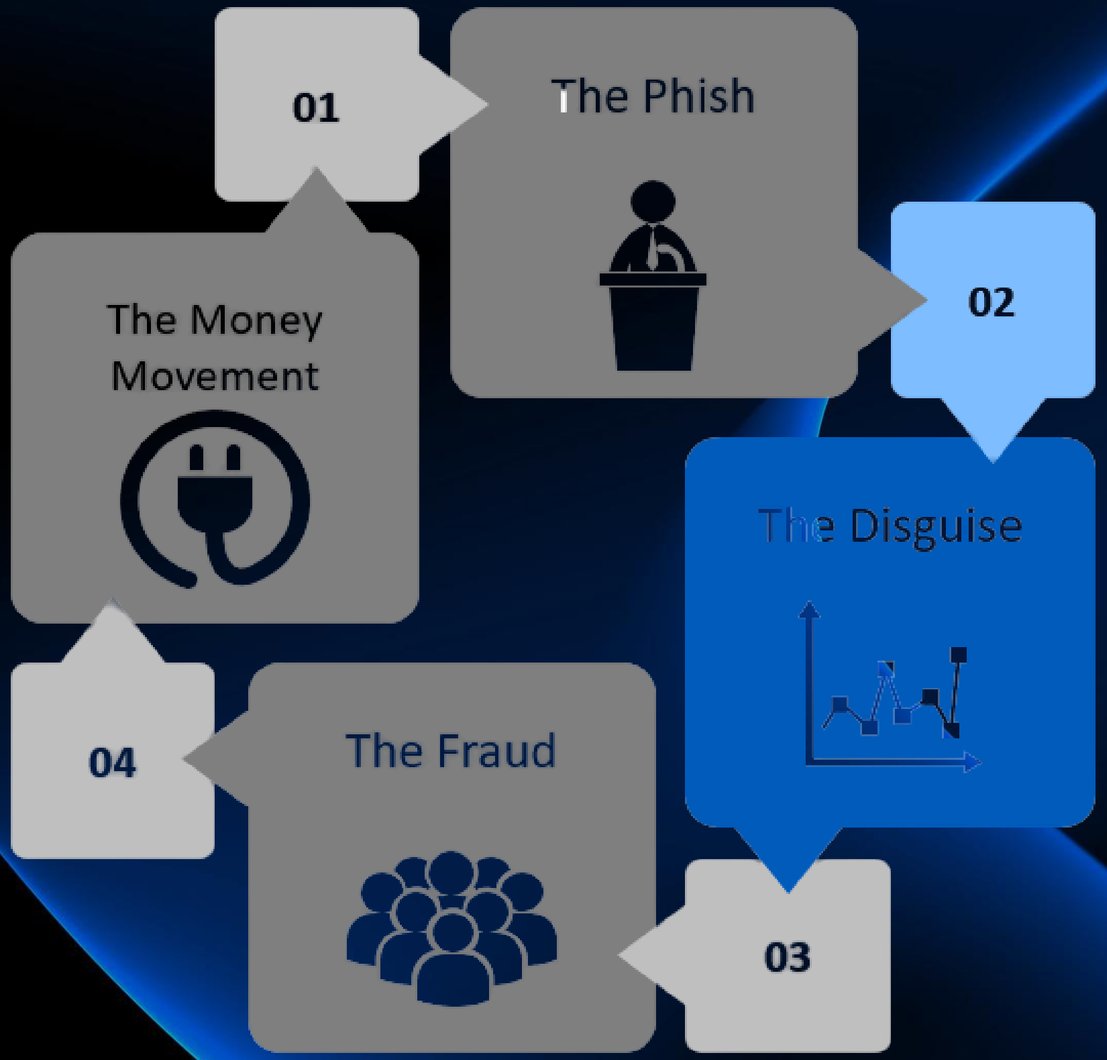
Phishing Example - BEC



The Phish

- ✓ A mass emailing to board base
- ✓ Because of its spam nature this is a high-quality endeavor and continues multiple times
- ✓ Email list probably purchased online of all CEOs, CFOs, AP managers, etc.
- ✓ “Are you at your desk? I need you to take care of a wire transfer for me”
- ✓ Email headers show that this return email will go to an overseas domain (click reply and see)
- ✓ Spam Techniques allow the fraudster to know if this email was ever viewed by the recipient, and if so this will generate more attempts

Phishing Example - BEC



The Disguise

- ✓ Creates mimicked domain name of the company and sets up email to match the CEO's name
  - ➢ **billgates@micros0ft.com**
- ✓ Or, if the fraudster can locate a personal email for the CFO (such as a Gmail) then they will create a mimicked Gmail email account
  - ➢ **billgates@gmail.com**
- ✓ Good hackers will look for "open mail relays" in the real company's exchange server

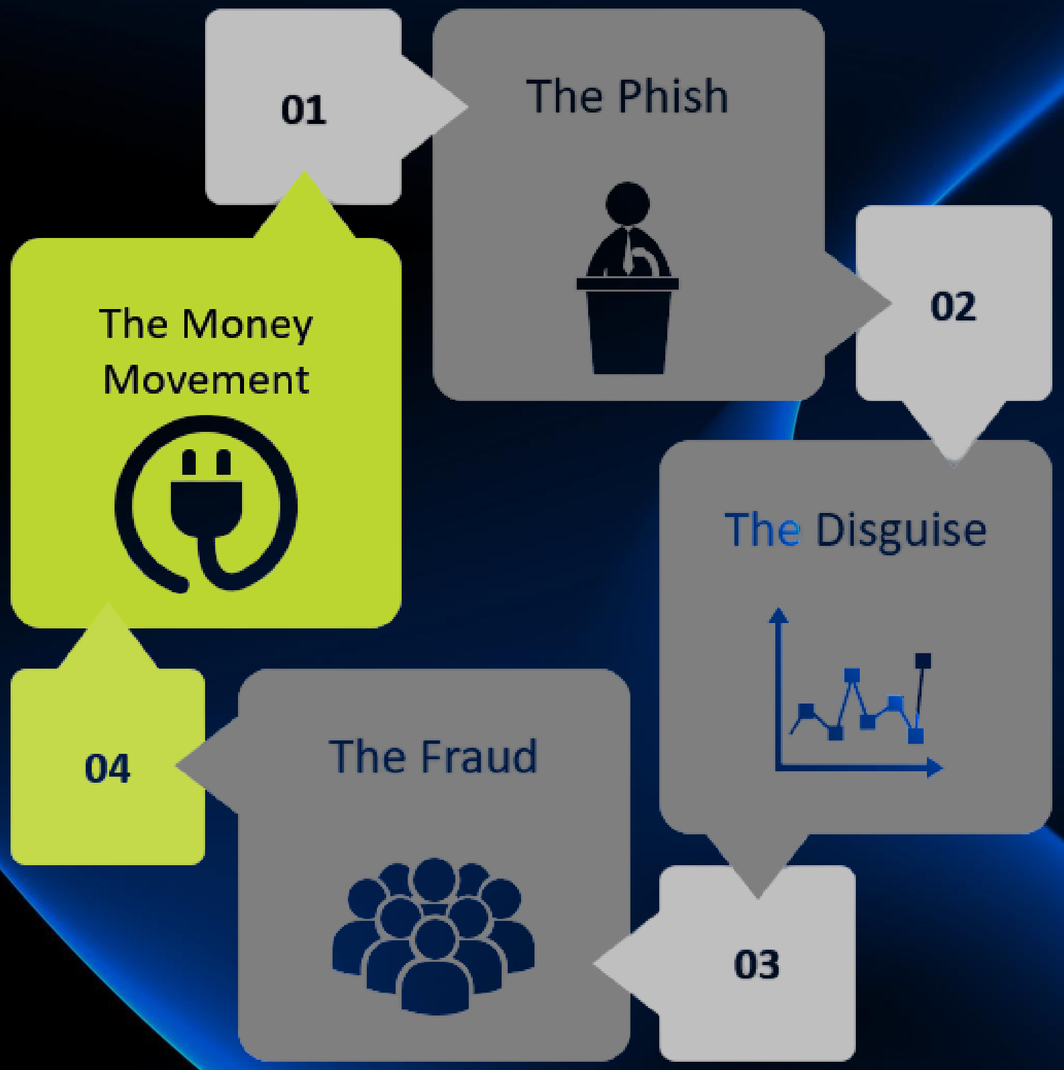
Phishing Example - BEC



The Fraud

- ✓ Asks for details or procedure for domestic wire transfer, in order to confirm that this target can send a wire, or if its another employee they should be targeting
  - ➢ “Jenn, Will you be able to process a wire transfer today before your meeting?”
- ✓ Fraudster will push for the request to be expedited
- ✓ Will inquire about the status multiple times and wants confirmation as soon as possible
- ✓ Fraudster will send an invoice from the compromised email
- ✓ The fraudulent invoice will say “bill it to expenses” or training, or something accounting related

Phishing Example - BEC



The Money Movement

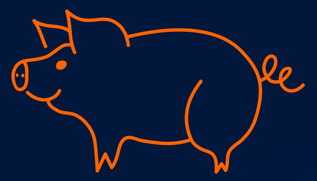
- ✓ Transaction Beneficiary is usually a money mule
- ✓ Mules are responsible for sending money to the next mule (Knowingly or unknowingly)
- ✓ Typical mule activity (re-wire overseas, Western Union)
  - ➢ Romance Scams and other confidence scams
  - ➢ Import/Export and third-party payment processors
  - ➢ Mystery Shoppers
  - ➢ Short Term Visa mules
- ✓ This step confounds law enforcement
- ✓ This step stops any wire recall attempts

Phishing Example - Pig Butchering

Phase	Timeframe	What Happens
Initial Contact	Day 1–3	Scammer sends a random or “wrong number” message via SMS/social media.
Relationship Building	Week 1–2	Daily conversations start; scammer builds rapport and appears successful.
Trust & Grooming	Week 2–4+	Scammer talks about crypto trading and shows fake profits; emotional bond grows.
Investment Pitch	Week 3–5	Victim is encouraged to “try investing” through a fake platform.
The Big Deposit	Week 4–6+	Victim is convinced to invest a large sum for high returns.
The Slaughter	Week 6+	Funds become inaccessible; scammer vanishes or asks for fees/taxes to withdraw.

Phishing Example - Pig Butchering

Pig Butchering Stats



$3.94 Billion Lost to Investment Scams in 2023

- According to the FBI IC3, Investment fraud was the highest-reported loss category, with pig butchering scams making up a significant portion of that total



Global reach and victims span the U.S., Canada, Europe, and Asia, but many scam operations are run out of cyber scam compounds in Southeast Asia, often involving human trafficking victims forced to run scams.



Average Individual Loss: $50,000 - $200,000

- Victims often lose life savings due to long-term grooming and fake returns



Check out Operation Shamrock and Founder and CEO Erin West



Spear Phishing Defined

Spear phishing is a targeted form of phishing in which the bad actor crafts a personalized message aimed at a specific individual, organization, or role within a company

How Spear Phishing Works?

1. **Research Phase** - Bad actor gathers details about the target (job title, contacts, recent projects, etc.) from LinkedIn, company website, or social media
2. **Email Crafting** - Creates a believable message tailored to the targets context (e.g., “Here’s the Q3 budget for review”
3. **Hook & Payload** - Includes a malicious link or attachment that installs malware or leads to a fake login page
4. **Execution** - Victim clicks the link, opens the file, or enters credentials giving the bad actor access to sensitive data and systems



Whaling Phishing Defined

Whaling is a highly targeted type of phishing attack aimed at high-level executives or individuals with access to sensitive company information like CEOs, CFOs, or legal counsel

How Whaling Phishing Works?

1. **Reconnaissance -** Bad actor researches the executive's role, company structure, and communication style. Information is gathered from social media, press releases, and corporate websites.
2. **Spoofed or Compromised Email** - Sends an email that appears to come from a trusted internal or external source (e.g., another executive, attorney, or vendor)
3. **High-Stakes Message** - Message may request an urgent wire transfer, confidential documents, or login credentials. Often uses fear, urgency, or authority to pressure the target
4. **Execution & Exploitation** - Once the victim complies, the bad actor may gain funds, sensitive IP, or access to internal systems



Angler Phishing Defined

Angler phishing is a social engineering attack that uses fake customer service accounts on social media to trick victims into sharing personal or financial information. These are common on platforms like X, Facebook, and Instagram. Bad actors target people already frustrated or looking for support from legitimate companies.



How Angler Phishing Works?

1. **Target the Victim -** The bad actor monitors posts or comments where users tag real companies
2. **Impersonating Support** - A fake account with a similar name and logo responds quickly, posing as official support
3. **Hooking the Victim** - The bad actor asks the user to click a link or direct message their login info, PIN, or other personal details
4. **Harvesting Data** - Victim unknowingly hands over sensitive information, which may lead to account takeover, identity theft, or financial fraud

Smishing Defined

Smishing (SMS Phishing) is a type of cyberattack where bad actors send fraudulent text messages to trick victims into clicking malicious links, sharing personal information, or downloading malware.

How Smishing Works?

1. **The Bait -** The victim receives a text claiming to be from a trusted source (e.g., a bank, delivery service, or government agency. Common messages would say “Your account is locked” or “Package undeliverable” or “Confirm this transaction”
2. **The Hook -** The message includes a link or phone number that leads to a fake website or prompts the user to respond
3. **The Trap -** Victim clicks the link or replies and unknowingly gives away personal info, credential, or installs malware
4. **The Exploitation -** Bad actor uses the stolen information to access accounts, commit fraud, or sell the data on the dark web



Vishing Defined

Vishing (Voice Phishing) is a type of social engineering attack where a bad actor uses phone calls or voice messages to trick victims into revealing sensitive information or performing actions that benefit the bad actor



How Vishing Works?

1. **Initial Contact -** The bad actor calls the victim or leaves a voicemail pretending to be from a trusted entity (e.g., IRS, bank, IT Support)
2. **Creating Urgency or Fear -** Common tactics include threats of account suspension, legal trouble, or fraudulent activity
3. **Information Extraction -** The victim is pressured to provide sensitive data like login credentials, credit card numbers, or verification codes
4. **Follow-Up Exploitation -** Bad actors may use the info immediately for fraud or guide the victim through actions like transferring money or installing remote access tools

Phishing Attack Quick Video

How phone scammers are using AI to imitate voices



Phishing Attack Prevention Strategies

- **Awareness Training**
  - Educate users on identifying phishing signs across all platforms
- **Multi-Factor Authentication**
  - Enable MFA on ALL financial and sensitive accounts
- **Email/SMS/Call Filtering**
  - Block suspicious messages, numbers & URLs



- **Social Media Monitoring**
  - Watch for fake customer service accounts
  - Make your social media accounts private
- **Limit Public Information**
  - Reduce what execs/employees share online to prevent targeted attacks

Phishing Attack Response Strategies

- **Isolate the Threat Immediately**
  - Disconnect affected devices from the network
  - Block malicious links, domains, or IP addresses in email and firewall systems

- **Notify Internal Teams**
  - Alert IT, Security, and management teams right away
  - Activate your incident response plan, if applicable

- **Reset Compromised Credentials**
  - Force password changes and invalidate session tokens for affected accounts
  - Apply MFA where not already enabled

- **Preserve & Analyze Evidence**
  - Save emails, headers, links, and user activity logs
  - Perform forensic analysis to determine the scope and method of attack

- **Notify External Stakeholders**
  - Inform customers, partners, vendors, and regulators if data was exposed, when needed
  - File a report with authorities (e.g., FBI IC3, FTC, or local PD

- **Clean & Restore Systems**
  - Remove malware or backdoors if present
  - Re-image or restore affected systems from clean backups



How many of you have heard of the term “Pig Butchering” before today?

SIM Swap

SIM Swap Define

SIM Swap fraud (also known as SIM Hijacking) is when a bad actor tricks a mobile carrier into transferring a victim’s phone number to a SIM card they control. This gives the bad actor access to calls, texts, and MFA codes, allowing them to take over bank, email, and crypto accounts.

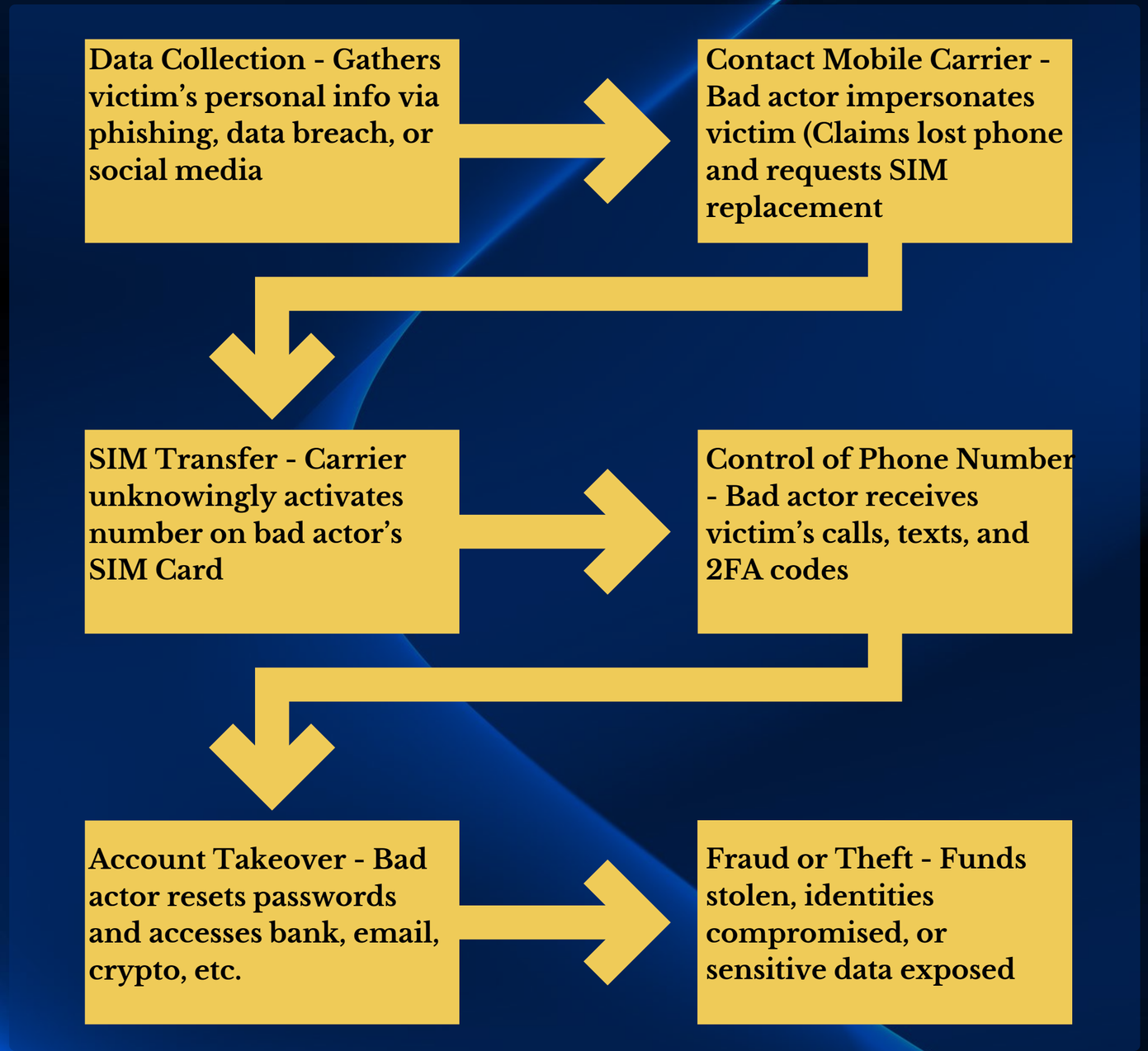
Mobile Numbers are a Top Target

6,000+ Complaints in a single Year - Complaints have doubled year-over-year

$72 Million in Losses (2023 - U.S. Alone)

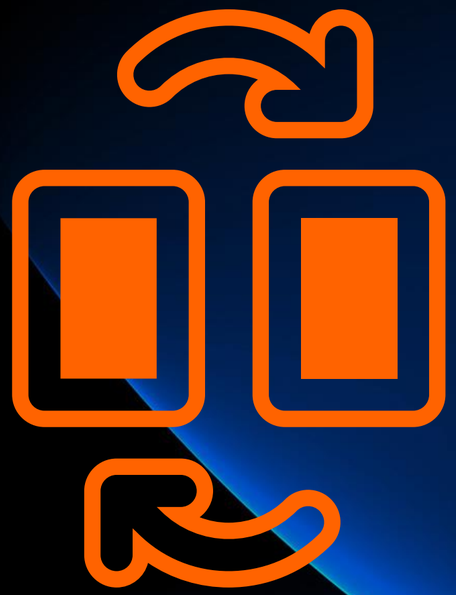
Average Individual Loss is $10K - $200K

SIM Swap Scheme



SIM Swap Prevention Strategies

- **Strengthen Two-Factor Auth**
  - Use app-based authenticators instead of SMS (Google Authenticator)
  - Consider hardware tokens for high-risk accounts
- **Implement Account Safeguards**
  - Set up account PINs or passwords with your mobile carrier
  - Enable SIM Swap alerts or port freeze options
- **Educate and Train Users**
  - Run awareness campaigns on SIM swap risks and social engineering tactics
  - Conduct simulated phishing & social engineering tests to improve vigilance



- **Monitor Account Activity**
  - Regularly review account activity and notify users of changes
  - Use anomaly detection systems to flag unusual login or transfer attempts
- **Collaborate with Service Providers**
  - Work closely with carriers to verify identity changes and monitor SIM swap requests
  - Report suspicious behavior promptly to the carrier and law enforcement

SIM Swap Response Strategies

- **Isolate the Threat Immediately**
  - Disconnect affected devices from the network
  - Temporary disable SMS notifications to prevent further code interception

- **Contact your Mobile Carrier**
  - Report the SIM Swap immediately to the carrier
  - Request immediate reversion and enhance account security (e.g., port freeze or additional PIN Verification

- **Secure Affected Accounts**
  - Reset passwords and invalidate sessions for accounts using the compromised number
  - Transition to more secure auth methods (MFA or Hardware tokens

- **Notify Financial Institution**
  - Alert your bank and other critical service providers about the unauthorized access
  - Monitor and flag unusual account activities

- **Preserve Evidence**
  - Save communications (texts, emails) with the carrier and service providers
  - Document any suspicious activity for investigation

- **Report to Authorities**
  - File a report with local LE and/or FBI’s IC3
  - Follow up with your credit agencies to monitor any potential fraud



How many of you have heard of SIM Swap fraud before today?

Injection Attacks

Injection Attacks Defined

Injection attacks are a type of cyberattack where a malicious actor inserts (or “injects”) harmful code or commands into a program or system to manipulate its behavior, steal data, or gain unauthorized access. These attacks exploit vulnerabilities in input handling especially when user input is not properly validated or sanitized.

Definitions

- **SQL -** Like a spreadsheet for storing and organizing data in rows and columns
- **NoSQL -** More flexible storage for messy or changing data (like documents or social media posts)
- **LDAP -** A phonebook for usernames, passwords, and who can access what
- **REST -** A simple way apps talk to each other over the web (like ordering food online
- **SOAP -** A more formal way for systems to exchange data, often used in big companies



Common Injection Attacks

- **SQL Injection**
  - Tricking a website into giving up secret info by typing sneaky commands into a search box or login field
- **Command Injection**
  - Forcing a computer to run harmful commands it was never supposed to
- **Cross-Site Scripting (XSS)**
  - Hiding bad code on a website so it runs when someone else opens the page
- **LDAP Injection**
  - Manipulating a login system by messing with how it checks usernames and passwords
- **XML Injection**
  - Adding fake or dangerous info into files used to transfer data between systems
- **NoSQL Injection**
  - Tricking newer, flexible databases to give access or change data by using clever input

Injection Attacks and Fraud Schemes

Account Takeover (ATO)

- **Attack Type:** SQL Injection
- **How:** Bypasses login or authentication mechanisms
- **Fraud Result:** Unauthorized access to user accounts
- **Impact:** Funds transfers, unauthorized purchases, identity theft

Payment Diversion & Manipulation

- **Attack Type:** SQL/Command Injection
- **How:** Alters payment processing or routing logic
- **Fraud Result:** Redirected payments, manipulated pricing
- **Impact:** Financial Losses, customer trust issues

Data Theft & Identity Fraud

- **Attack Type:** SQL Injection, LDAP Injection
- **How:** Extracts PII. payment card info, credentials
- **Fraud Result:** Fake accounts, synthetic identities, phishing
- **Impact:** Regulatory fines, reputational damage

Injection Attacks and Fraud Schemes

Business Email Compromise (BEC)

- **Attack Type:** Cross-Site Scripting (XSS)
- **How:** Hijacks email sessions via injected scripts
- **Fraud Result:** Invoice fraud, payroll diversion
- **Impact:** Loss of funds, internal trust breakdown

Loyalty/Rewards Fraud

- **Attack Type:** SQL Injection
- **How:** Tampering with reward point balances or redemption systems
- **Fraud Result:** Unauthorized redemptions, point theft
- **Impact:** Financial Losses, customer trust issues

Healthcare or Insurance Fraud

- **Attack Type:** SQL/XML Injection
- **How:** Alters or submits fake medical claims
- **Fraud Result:** Illegitimate reimbursements, policy abuse
- **Impact:** Billing errors, increased premiums, regulatory scrutiny

Recent Injection Attacks



Recent Injection Attacks



Injection Attacks Preventative Strategies





- **Validate and Sanitize Input**
  - Only allow expected data formats (e.g., no code or special characters
- **Use Parameterized Queries**
  - Prevents attacks from injecting code into database queries
- **Employ Web Application Firewalls**
  - Blocks suspicious activity and common attack patters
- **Limit User Permissions**
  - Ensure accounts have only the access they truly need
- **Keep Software Updated**
  - Patch known vulnerabilities in apps, databases, and frameworks
- **Educate Developers in Secure Coding**
  - Anti-vulnerability minimization needs proper training in secure coding practices



Injection Attacks Response Strategies



- **Detect and Log Abnormal Activity**
  - Monitor for unusual queries, traffic, or system behavior
- **Isolate Affected Systems**
  - Immediately contain the breach to prevent spread
- **Conduct a Forensic Investigation**
  - Determine how the attack occurred and what was accessed
- **Notify Impacted Parties**
  - Comply with breach notification laws and maintain transparency
- **Review and Strengthen Controls**
  - Apply lessons learned to update policies and protections



What’s one thing you can do today to reduce the risk of injection attacks in your environment?



THANK YOU

John Fick, MLS, CFE, CFCI, CECFE
Director of Fraud - Northwest Bank

John.Fick@Northwest.com
469.400.2885