

# NAM-CSIRT Social Engineering Awareness

**Ms. Cornelia Shipindo**  
**Executive NAM-CSIRT**

**13 October 2026**



# OVERVIEW

---

**About NAM-CSIRT**

---

**What is Social Engineering**

---

**How Social Engineering Works**

---

**Types of Social Engineering Attacks**

---

**Common Warning Signs**

---

**Digital Fraud and Consumer Scams**

---

**Six Steps of Vishing**

---

**Responding to Social Engineering Attacks**

---

**Importance of Cybersecurity Awareness Training**

---

**Conclusion**

---

# ABOUT NAM-CSIRT



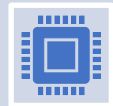
Namibia Cyber Security Incident Response Team (NAM-CSIRT) serves as a national central point of response to cyber incidents & coordination.



Bringing together cybersecurity collaboration of government agencies, private companies, and international partners.



Standing as a central hub for collecting, analyzing, and disseminating threat intelligence while enabling proactive security measures.



NAM-CSIRT facilitates local, regional and international collaboration of information sharing on cybersecurity threats.



NAM-CSIRT protect, respond, coordinates, share cybersecurity awareness and advisories.



NAM-CSIRT encourages all organization to report incident to ensure effective coordination and response support.



NAM-CSIRT Constituents benefit from cyber expertise, incident coordination & support, access to security advisories and response guidelines.

## What Is Social Engineering?

---

Social engineering is the psychological manipulation of people by tricking them into revealing confidential information, transferring money, or performing unsafe actions that compromise their security.



## How Social Engineering Works:

### TRUST

- By impersonating a familiar person or organisation.

### UEGENCY

- Creating pressure to act immediately.

### FEAR

- Threatening consequences or account closure.

### COURIOSITY

- Using tempting links, files or stories.

### HELPFULNESS

- Asking someone to “assist” with an unusual request.

## Types of Social Engineering Attacks:

---

**Phishing:** fraudulent emails designed to steal information or deliver malware.

---

**Spear phishing:** highly targeted messages using personal or organisational details.

---

**Smishing:** malicious requests sent by SMS or messaging applications.

---

**Vishing:** fraudulent voice calls that pressure victims to disclose personnel information.

---

**Pretexting:** a fabricated story used to obtain data or access.

---

**Baiting:** an attractive offer, download or device used as a trap.

---

**Tailgating:** following an authorised person into a restricted area.

# Social Engineering Red Flags



## FROM

- I don't recognize the sender's email address as someone I **ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- I **don't know the sender personally** and they **were not vouched for** by someone I trust.
- I **don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.



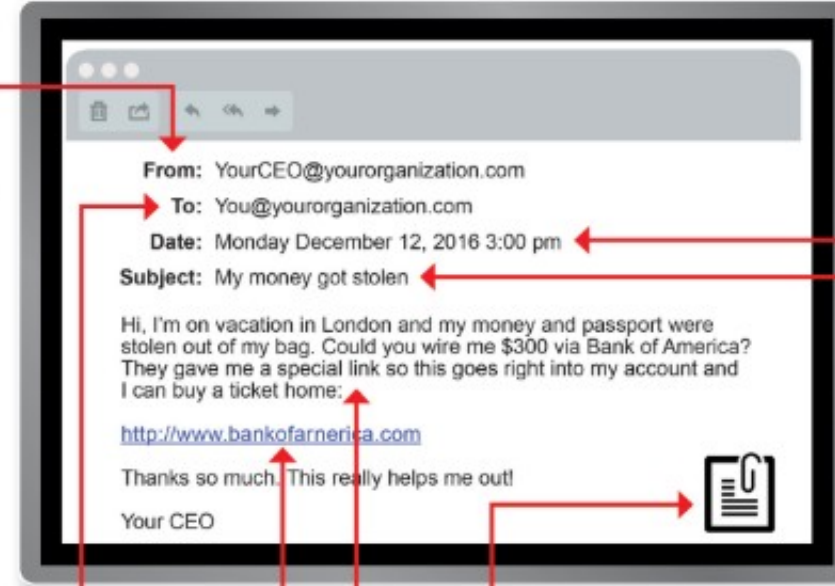
## TO

- I was cc'd on an email sent to one or more people, but I **don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.



## HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big red flag**.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, [www.bankofamerica.com](http://www.bankofamerica.com) — the "m" is really two characters — "r" and "n."



## DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?



## SUBJECT

- Did I get an email with a subject line that is **irrelevant or does not match** the message content?
- Is the email message a reply to something I **never sent or requested**?



## ATTACHMENTS

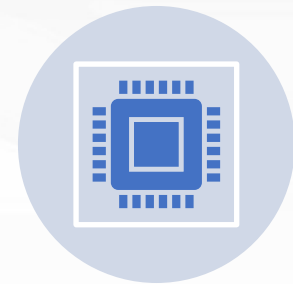
- The sender included an email attachment that I **was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt** file.



## CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar or spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd or illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

## Common Warning Signs:



An unexpected request for passwords, one-time PINs, money or confidential information.



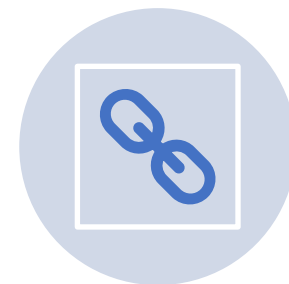
A message that creates unusual urgency, secrecy or fear.



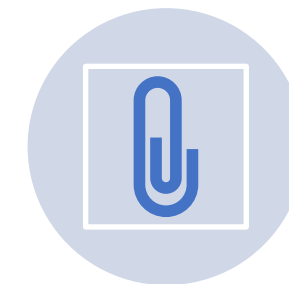
A sender address, domain name or caller identity that does not match expectations.



Generic greetings, unusual wording, spelling errors or inconsistent branding.



Links whose destination differs from the displayed text.



Unexpected attachments, QR codes or login pages.



A request to bypass normal approval or security procedures.

# Email and Messaging Safety

Use strong, unique passwords and multi-factor authentication.

Check the full sender address and not only the display name.

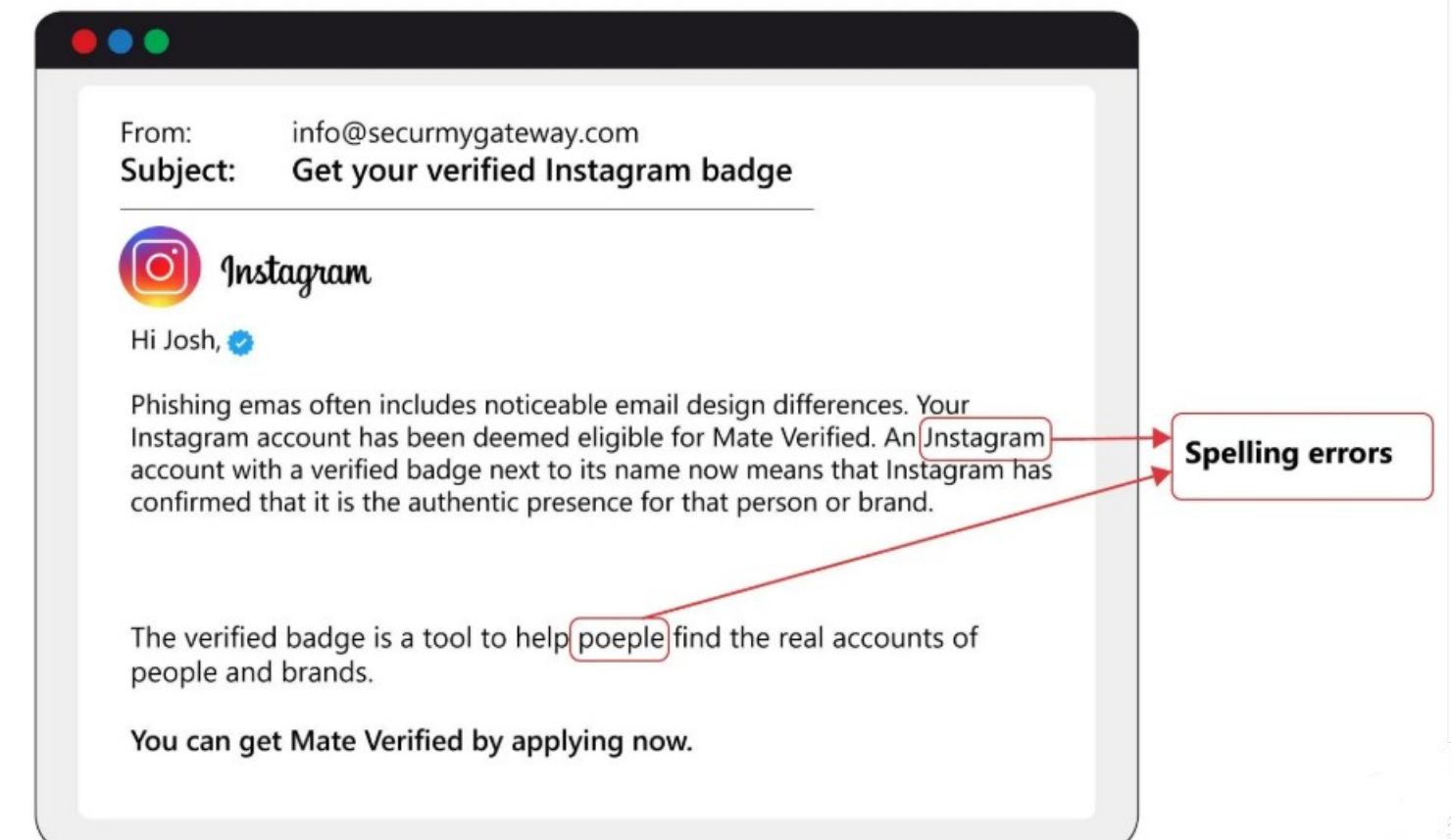
Hover over links before opening them and avoid shortened or unfamiliar links.

Do not open unexpected attachments or enable macros.

Be cautious with QR codes that lead to login or payment pages.

Always confirm unusual financial, credential or data requests using a different channel.

Immediately report suspicious emails or texts to relevant authorities.



## Digital Fraud and Consumer Scams:

Banking fraud losses rose sharply from N\$8.7 million in 2020 to over N\$54 million in 2024

Increasing to N\$79 million by end of 2025, according to the Bank of Namibia

Fraudsters increasingly rely on deepfakes and voice cloning

Using counterfeit banking applications and phishing links

As well as vishing to exploit psychological panic

# The Six Stages of Vishing



## Six Steps of Vishing:

---

**1. Reconnaissance:** The attacker starts by gathering data about the target victim, including names, job titles, phone numbers, banks used, and internal company procedures. Attackers often choose victims who are easy to pressure, such as seniors or people who have just applied for a loan or credit card.

---

**2. Pretexting and Caller ID Spoofing:** The attacker builds a believable yet fake scenario, also known as a pretext, such as an urgent bank alert, a KYC update, or an IT support ticket. Caller ID spoofing software or Voice over Internet Protocol (VoIP) services make the phone number appear legitimate, such as a bank helpline, a government office, or a known company.

---

**3. Establishing Contact and Impersonation:** The victim receives an unexpected call or voicemail. In some cases, the attacker first sends a text or email that prompts the victim to call a specific number. This is known as telephone-oriented attack delivery (TOAD). On the call, the attacker poses as a bank fraud officer, KYC executive, tax official, or IT support agent and asks for details like the victim's name, loan amount, or credit card type to seem legitimate.

## Steps of Vishing:

---

**4. Generating Urgency or Fear (Social Engineering):** After gaining trust, the attacker creates urgency, fear, or excitement to manipulate the victim into taking a specific action. Typical claims include a blocked bank account, a suspicious transaction, expired KYC, unpaid taxes, a pending refund, or the threat of legal action. The goal is to trigger an emotional response that discourages the victim from verifying the request independently.

---

**5. Extract Credentials, Data or Access:** When the victim is anxious and compliant, the attacker requests the credentials, information, or access they are after. This could be a password, card number, CVV, or one-time password (OTP). They may also ask the victim to approve a verification request or a multi-factor authentication (MFA) push notification. In an MFA fatigue attack, the fraudster sends repeated prompts until the victim approves one.

---

**6. Fraud Implementation:** With the information or access, the attacker either removes the money or gets into the company network. Funds are usually transferred through several accounts within minutes, making them hard to trace and recover. In corporate scenarios, the stolen access could be used for data theft or further attacks.

## Phone and In-Person Safety

---

Do not disclose sensitive information solely because a caller sounds confident.

---

Ask for identification and verify it through an official contact point.

---

Never allow unknown individuals to follow you into restricted areas.

---

Challenge or report unattended visitors according to organisational procedure.

---

Protect conversations, screens, documents and access cards in public spaces.

---

Do not connect unknown USB devices or other removable media.

---



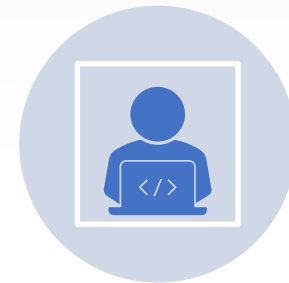
## Responding to Suspicious Attacks:

|         |                                                                              |
|---------|------------------------------------------------------------------------------|
| Stop    | Do not respond, click, download, scan or approve immediately.                |
| Verify  | Contact the person or organisation using a trusted, independent channel.     |
| Inspect | Check the sender, link destination, attachment type and context.             |
| Protect | Never share passwords or one-time PINs; use approved systems and procedures. |
| Report  | Notify the designated cybersecurity or ICT contact promptly.                 |

## Reporting Suspicious Activities:



Immediately stop interacting with the message, caller or website.



Report to your organisational IT or Cybersecurity representatives.



Preserve relevant evidence, such as the email, screenshot, phone number or URL.



Escalate matter to relevant and applicable authorities and regulators



Do not feel embarrassed, early reporting helps limit harm.



Change affected credentials from a trusted device to reduce impact.

## Report Cyber Frauds, Threats & Incidents:

---

The NAMPOL station closest to you.

---

Contact your banking institution helpline or branch

---

Inform your SIM card service provider (MTC, TN mobile)

---

Child-life online via **info@lifeline.org.na**

---

Central bank via **illegalschemes@bon.com.na**

---

NAM-CSIRT via **report@nam-csirt.na**

## Cybersecurity Awareness and Training:

### Human Factor Importance

- Human factors are essential in cybersecurity, requiring awareness to reduce risks and improve defenses.

### Technical Staff Training

- Technical staff need specialized skills to detect and respond effectively to cybersecurity incidents.

### Non-Technical Staff Awareness

- Non-technical staff require training to recognize common threats like phishing and social engineering attacks.

### Continuous Training Benefits

- Ongoing training keeps skills updated as threats evolve, reducing fraud and incident impacts and improving security posture of organizations and overall landscape of Namibia.

## Conclusion:

Social engineering targets human behaviour and not only technology.

Urgency, fear, trust and curiosity are common manipulation techniques.

Unexpected requests must be independently verified.

Passwords and one-time PINs must never be shared with anyone.

Prompt reporting protects you and the organisation.

Think before you click. Verify before you trust. Report before damage spreads.

# Q & A



[www.namcsirt.na](http://www.namcsirt.na)



+264 61 222 666



[info@nam-csirt.na](mailto:info@nam-csirt.na)

