Ongoing Threat Trends & Real Case Studies

Introduction to Emerging Phishing Threats

- Phishing attacks continue evolving with new delivery channels and techniques.
- Attackers use automation, AI, and social engineering to increase success rates.
- Learning real cases helps us avoid real mistakes.

Trend 1: AI-Generated Phishing

- Attackers now use AI to write perfect emails.
- No spelling mistakes → harder to detect.
- Messages sound more personal and real.

Trend 2: Deepfake Voice Phishing

- Attackers use voice-cloning to sound like someone you trust.
- Mostly used for financial fraud.

Trend 3: Social Media Phishing

- Fake giveaways
- Fake job offers
- Fake pages copying real brands

Attackers use your posts to tailor their messages.

Trend 4: QR Code Phishing (“Quishing”)

- Fake posters with QR codes
- Fake “payment QR codes”
- QR codes in emails leading to login pages

People trust QR codes more → attackers exploit this.

Trend 5: Multi-Platform Attacks

Attackers might start on:

- Instagram → move to Email
- Email → move to WhatsApp
- WhatsApp → move to Fake Forms

They mix platforms so users feel less suspicious.

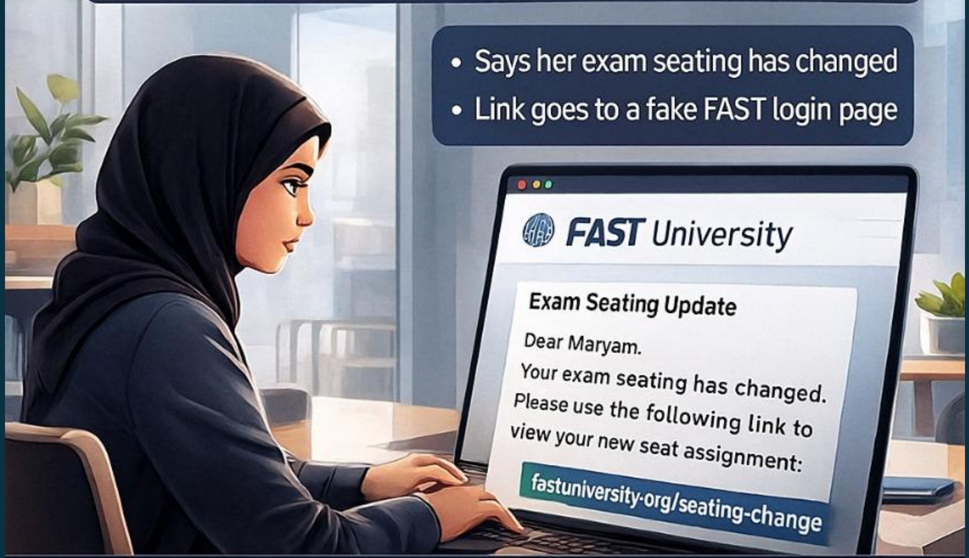
QR Code Phishing (Quishing)

- Attackers place malicious QR codes in public places or digital flyers.
- Scanned QR directs users to credential-harvesting pages.
- Hard to visually verify legitimacy before scanning.
- Rising trend in workplaces using QR-based authentication.

Real Case: FAST University Student

(Scenario)

! Maryam receives an email pretending to be from "FAST Examination Office":



- Says her exam seating has changed
- Link goes to a fake FAST login page

FAST University

Exam Seating Update

Dear Maryam.

Your exam seating has changed. Please use the following link to view your new seat assignment:

fastuniversity-org/seating-change

✓ Says her exam seating has changed

FAST University

LegnLogn

Username

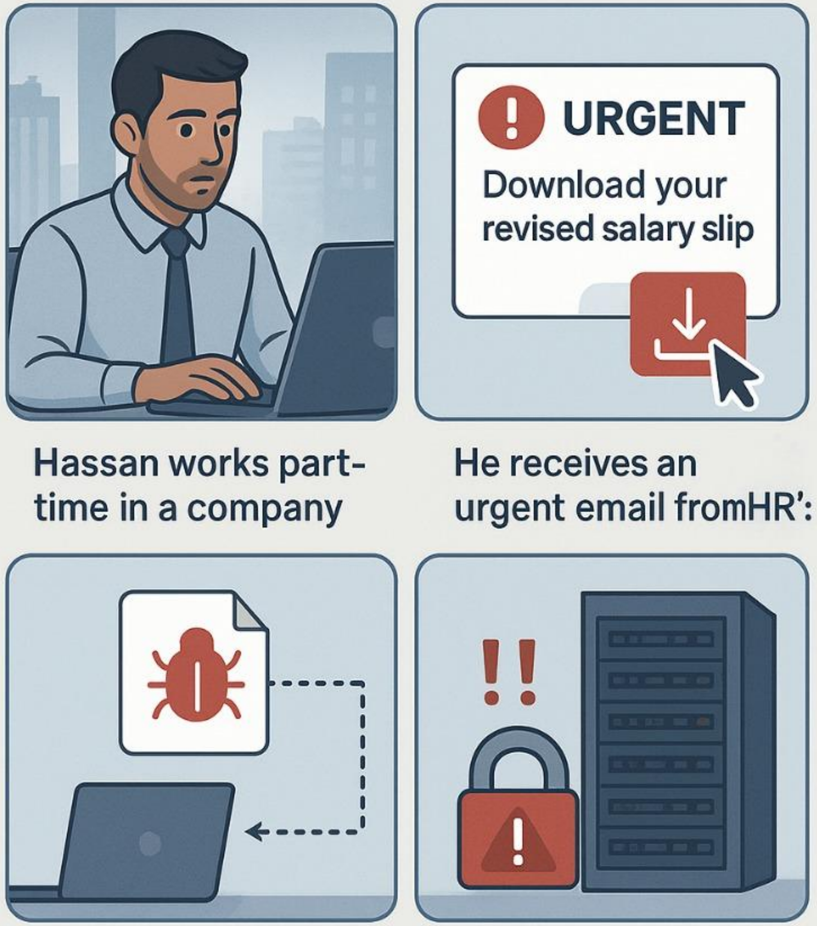
Password

fastuniversity-arg/agin-cheeo

✓ Unk enters her credentials

⚠ **Lesson:** Always check official university emails carefully

Corporate Employee
(Scenario)



Hassan works part-time in a company

He receives an urgent email fromHR':

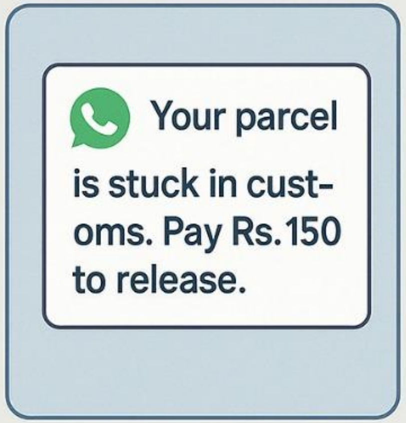
He downloads the file → malware infects his system

Huge downtime

LESSON: Never download attachments from unexpected or urgent emails — verify with HR directly

Real Case:
Social Engineering Attack

Arham gets a WhatsApp message



Your parcel is stuck in customs. Pay Rs.150 to release.

He pays through a fake link

Attackers now have his debit card info

Attackers now have his debit card info

LESSON: Small payments are used to trick users into bigger losses

How to Protect Yourself From New Threats

- Stay updated on new phishing techniques.
- Think before you click.
- Verify suspicious messages by calling trusted numbers.
- Use MFA everywhere.
- Never trust links sent through multiple platforms.
- If unsure → report to IT/security team.

Key Takeaway

Phishing is evolving, but one rule never changes:

Attackers succeed when you act quickly without thinking.

Pause. Verify. Stay safe.

Future Threat Outlook

- More AI-powered impersonation attacks on executives and finance teams.
- Increased targeting of authentication apps and MFA fatigue attacks.
- Growth in supply-chain phishing exploiting vendor relationships.
- Organizations must invest in continuous training and adaptive defenses.