Phishing Attacks: Spotting and Avoiding Scams

Protect yourself from deceptive online threats

$4.8B lost to phishing in 2023 (FBI IC3 Report)

83% of organizations experienced phishing attacks

Understanding Phishing and Social Engineering

→ Phishing

Deceptive emails, websites, or messages stealing info

→ Social Engineering

Manipulating people to reveal confidential data

→ Common goals

Steal credentials, financial info, install malware

→ Techniques

Urgency, fear, authority, trust

Email Phishing: Red Flags

- Generic greetings ("Dear Customer")
- Grammatical errors and typos
- Suspicious links or attachments
- Requests for personal information
- Threats or urgent deadlines
- Example: Fake invoice with malware

Website Phishing: Spotting Fake Sites

Check HTTPS and padlock

Secure connection indicates legitimacy

Verify domain spelling

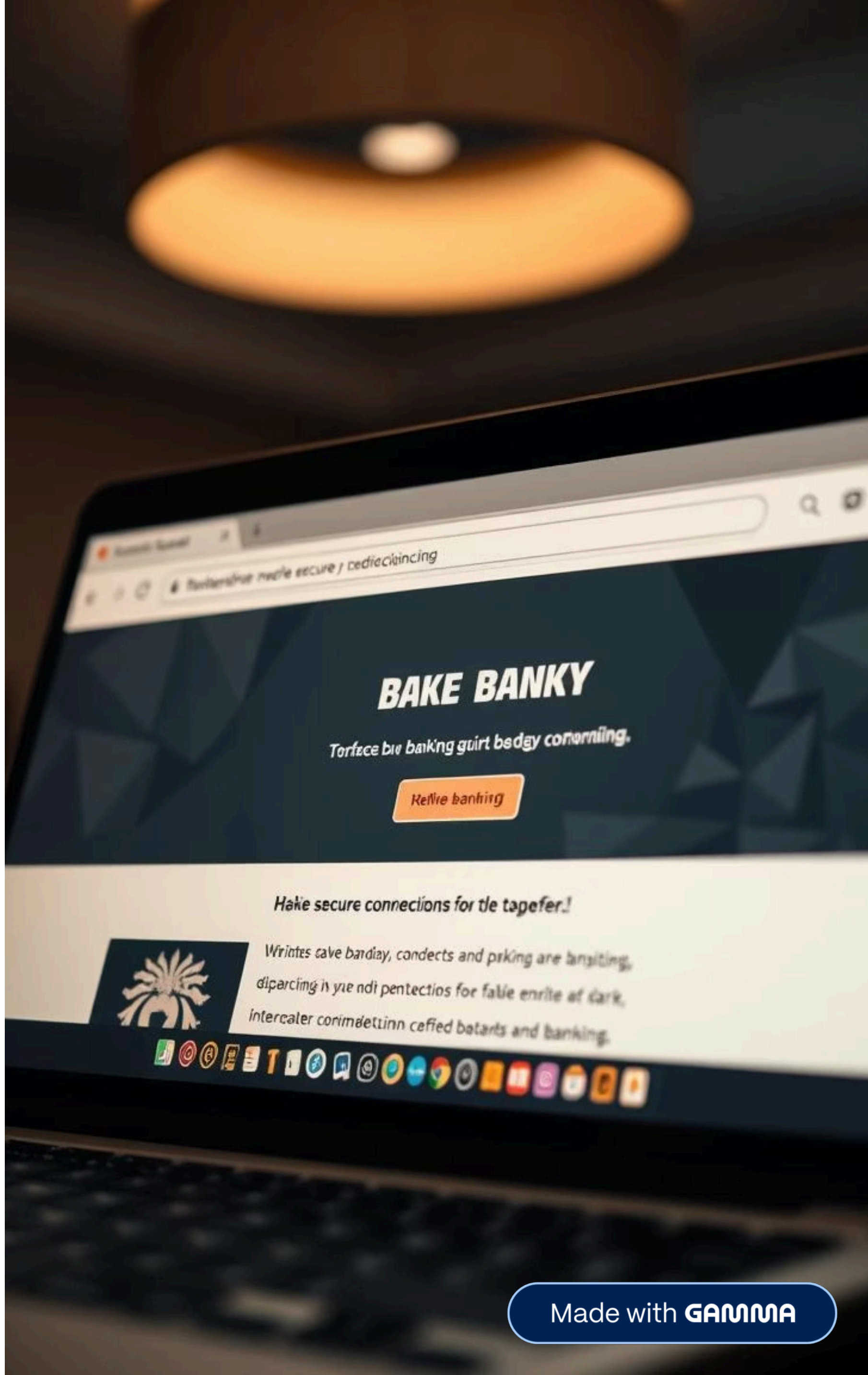
Watch for subtle misspellings

Use WHOIS lookup

Confirm ownership details

Inspect design consistency

Look for branding mismatch


BAKE BANKY
Torfzce bıı baıKng guirt bsdgy corıerniing.
Refire banhing
Hake secure connections for tle tapefer.!

Spear Phishing: Targeted Attacks

1

Personalized emails

Directed at specific individuals

2

Data sources

Social media, data breaches used

3

Fake colleagues or superiors

Impersonation to gain trust

4

Example

CEO fraud requesting wire transfer

Smishing and Vishing: SMS and Voice Phishing

Smishing

Phishing via text messages

- Fake prize offers
- Urgent requests

Vishing

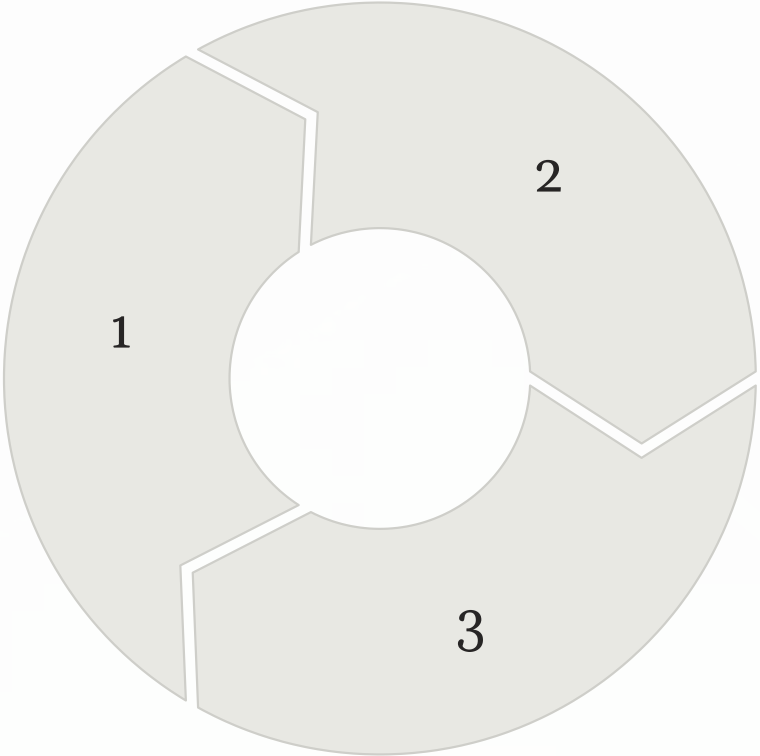
Phishing via phone calls

- Impersonating authorities
- Fake customer support

Social Media Phishing: Fake Profiles and Scams

- → Fake profiles gather info
- → Contests and quizzes steal data
- → Malware disguised as content
- → Example: "Free vacation" survey scam

Multi-Factor Authentication (MFA)



Extra security layer

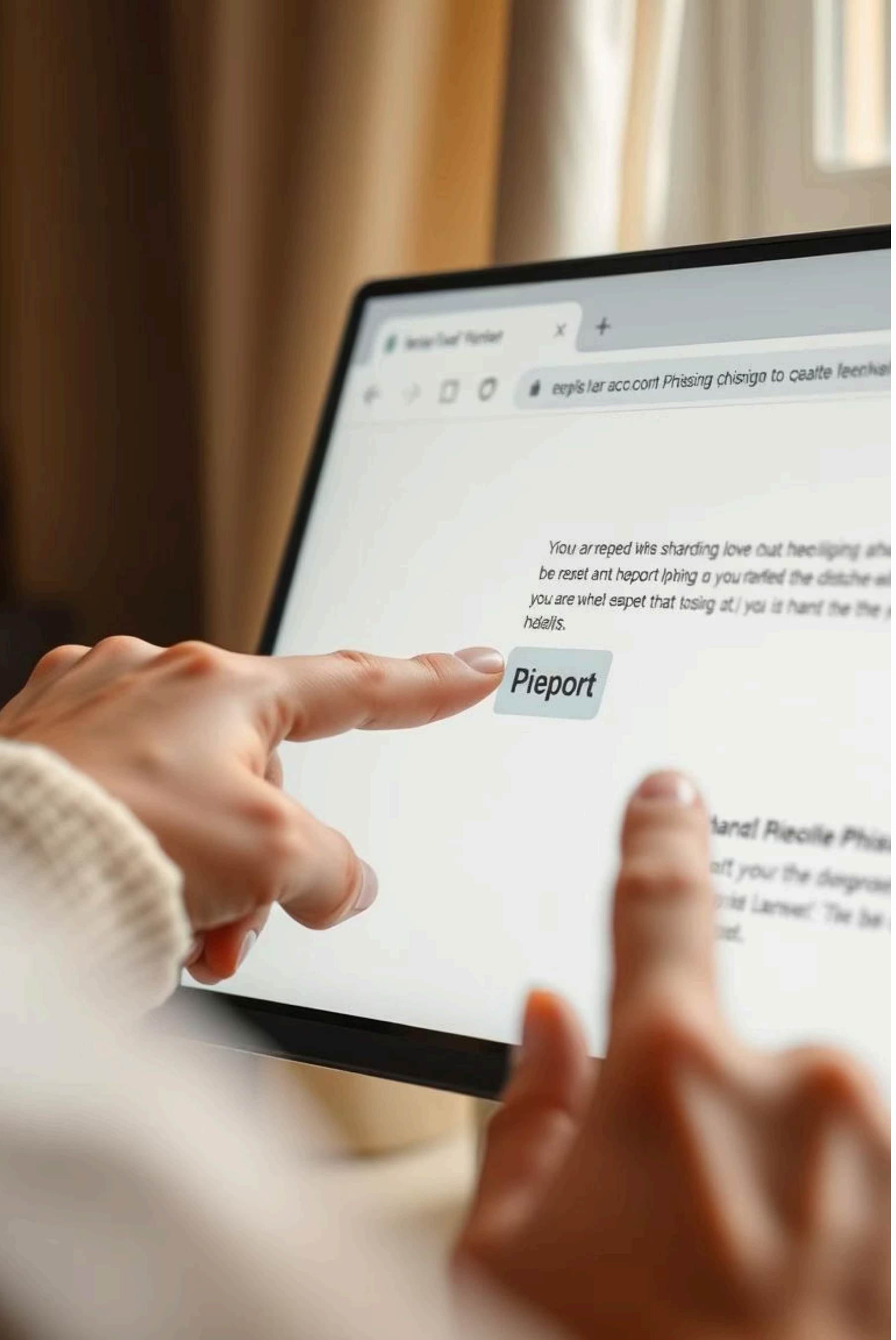
Reduces unauthorized access risk

Authentication methods

Apps, security keys, biometrics

MFA effectiveness

Blocks 99.9% of automated attacks



Verify and Report Suspicious Activity

Verify requests

Use official communication channels

Report phishing

Notify IT or security teams

Use anti-phishing tools

Browser extensions and software

Check site certificates

Confirm website security

Stay Informed and Vigilant

Learn latest tactics

Stay updated on phishing trends

Keep software updated

Patch vulnerabilities promptly

Trust instincts

If suspicious, be cautious

Enable browser protection

Activate phishing filters