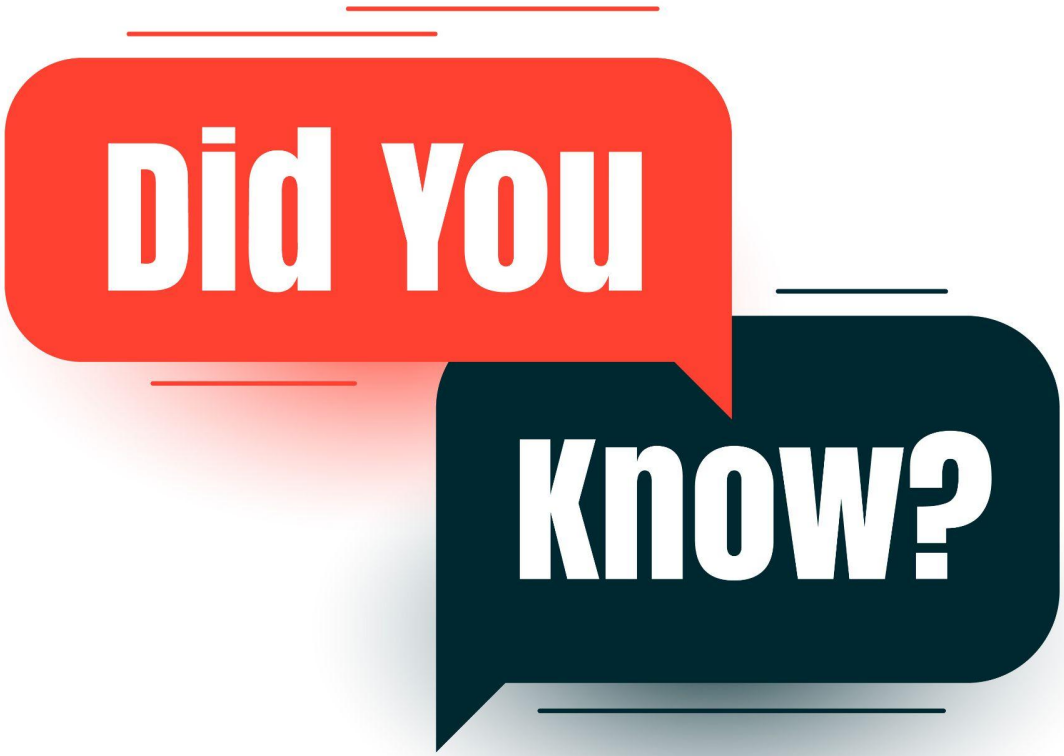
AMRITA
VISHWA VIDYAPEETHAM

PHISHERS ARE GETTING SMARTER- ARE YOU?

Neena Nithin

Faculty Associate, Amrita center for cyber security

AMRITA CENTER
FOR CYBER SECURITY
SYSTEMS & NETWORKS



According to the studies, 91% of the cyber attacks starts with a Phishing Email…

Table of contents

01
Phishing

Phishing is a type of online scam where criminals use fake emails or websites to trick people into giving them sensitive information, such as passwords or financial details.

02

Types of Phishing

All you need to know...

- Clone Phishing
- Spear Phishing
- Phone Phishing (Vishing)
- Smishing
- Pharming
- Scareware
- Typosquatting

Clone Phishing

This type of phishing involves creating a duplicate of an existing legitimate email and using it to trick the recipient into providing sensitive information.

Spear Phishing

This type of phishing targets specific individuals or organizations, often using personalized messages that are tailored to the recipient in order to make the attack more convincing.

Vishing

This involves using phone calls or voice messages to trick victims into providing sensitive information or taking actions that benefit the attacker.

Smishing

This type of phishing involves sending fake text messages to trick people into providing sensitive information.

Pharming

This type of phishing involves redirecting victims to fake or malicious websites without their knowledge or consent. This can be done by DNS poisoning or other technique

Scareware

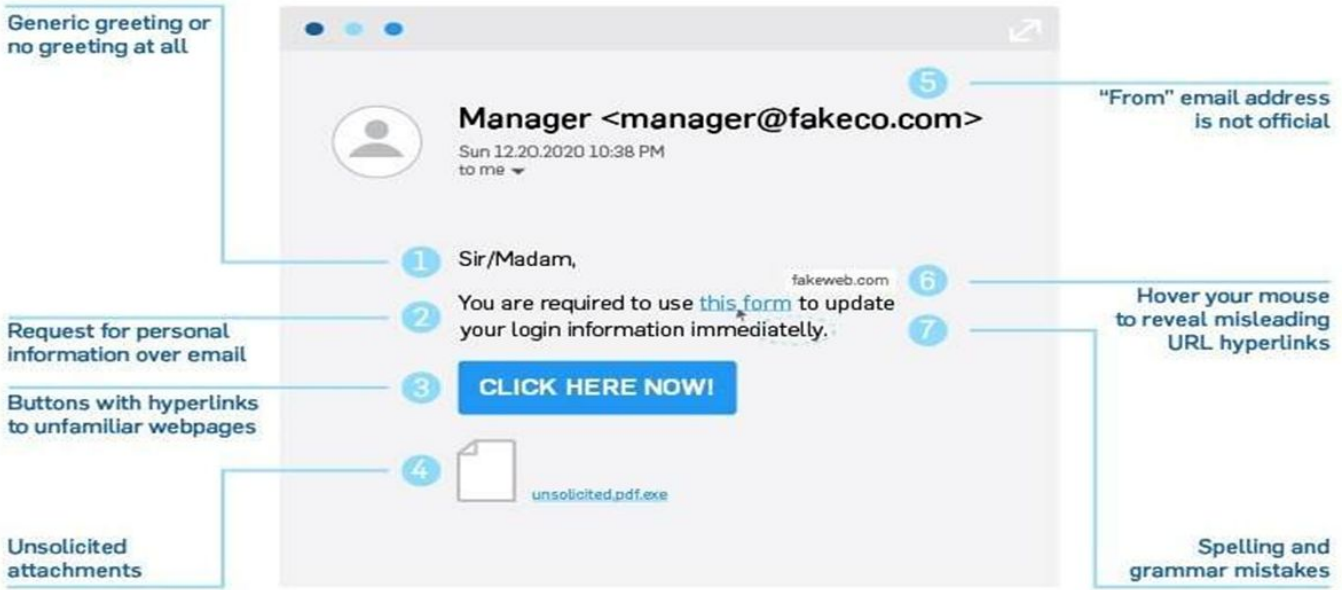
This type of phishing uses fake pop-up messages or alerts to trick victims into downloading or purchasing fake or malicious software.

Typosquatting

This type of phishing involves registering fake or misspelled version of popular websites to trick victims into visiting these sites and providing sensitive information or downloading malware.

securitymetrics

7 Signs of a Phishing Email



From: Amazon<management@mazonindia.in> Note an A is missing in Amazon

To: joey@gmail.com

amazon

Dear Client, Generic non- personalized greeting

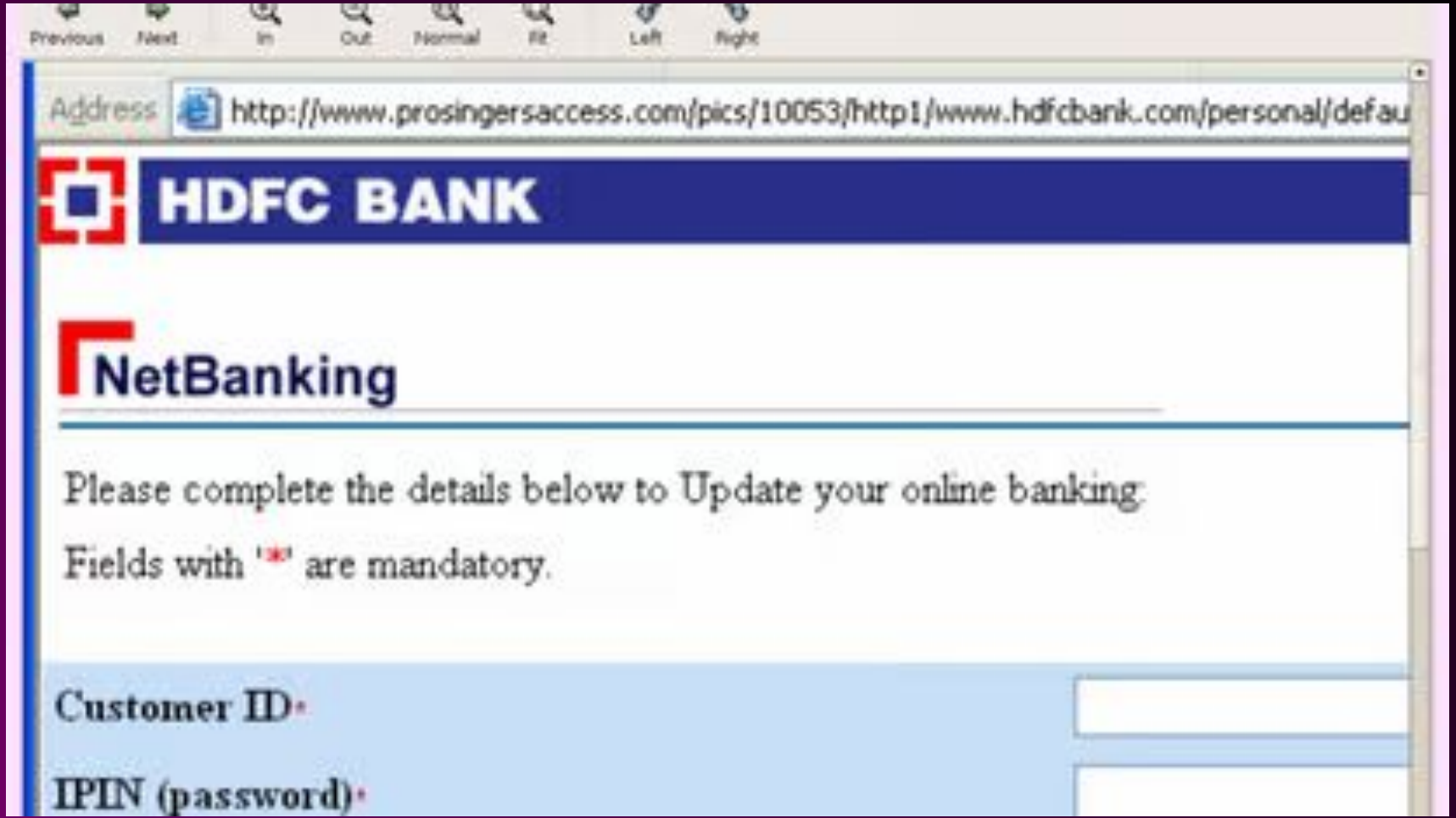
We have sent you this email, because we have strong reason to believe, your account has been used by someone else. In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter. We've locked your Amazon account and you have 36 hours to verify it, or we have the right to terminate it.

https://www.amazon.com/exe/dos/sign-in.html

http://redirect.kereskedj.com

Hovering over the link it points to another link which is not an Amazon site

Sincerely,
The Amazon Associates Team


Previous
Next
In
Out
Normal
Fit
Left
Right
Address
http://www.prosingersaccess.com/pics/10053/http1/www.hdfcbank.com/personal/defau
HDFC BANK
NetBanking
Please complete the details below to Update your online banking
Fields with '*' are mandatory.
Customer ID*
IPIN (password)*

04

Confidential information

Think twice before sharing...

- One-Time-Password (OTP)
- Credit/debit card number
- The card’s CVV number
- Expiry date
- Secure password
- ATM pin
- Internet Banking login ID and password and other personal information

05

How to stop

Thank you

Do you have any questions?

neenarmohan@gmail.com