



Phishing Awareness Training

Shreya R Deokar

*CAN YOU FIND
THE THE MISTAKE?*

Phishing

- Scammers pretend to be someone you know and like, such as a friend, family member, or company, to trick you into doing something you wouldn't normally do.



7 Types of Phishing Scams You Should Know About

Email Phishing Scams



It can appear to be an email from your CEO, Google, Paypal, Amazon, or even your bank.

1 Sender Email
Email domain is not official @google.com

2 Alert for immediate action
Scams push for quick action under emotion. Instead, pause and look for red flags.

3 Redirect
Hover over button reveals bit.ly link instead of official site

Subject: **Critical security alert for your linked Google Account**
From: **1 Google** <google@team-support.net>



2 Sign-in attempt was blocked for your linked Google Account
shellyteague@gmail.com

Someone just used your password to try to sign in to your account from a non-Google app. Google blocked them, but you should check what happened. Review your account activity to make sure no one else has access.

3 [Check activity](#)

You received this email to let you know about important changes to your Google Account and services.
© 2021 Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

Smishing scams



- **Phishing scams via text messages are these. Criminals are aware that individuals reply to texts and instant messages more quickly than to emails.**

Spear Phishing Scams

→ **This is when they specifically aim to harm you. They have done their homework on you, and they are aware of your work location, administrator, and relatives. There is a higher probability of fooling you.**

Spear Phishing in Action



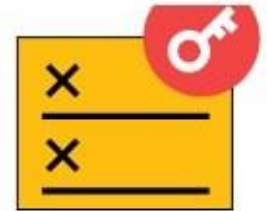
Threat actor
identifies a
target



Sends
legitimate-
looking email



Victim opens the
email containing
malware



Hacker gains
access to steal
data

Google Search Scams

→ **You might be shocked to learn that phishing links appear in some of Google's top search results.**

→ **In an effort to place their scam sites among the top search results, scammers also heavily invest in search engine optimization.**

Search Result Shows Brand

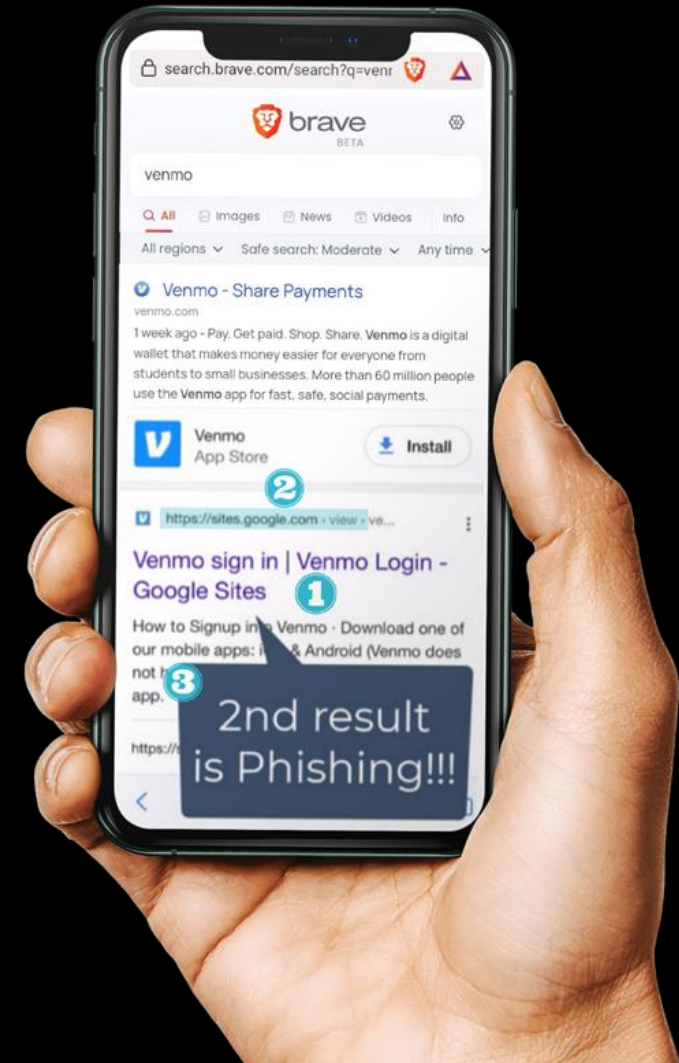
Title displays correct brand name

URL Mismatch

Title says Venmo but URL is a generic sites.google.com

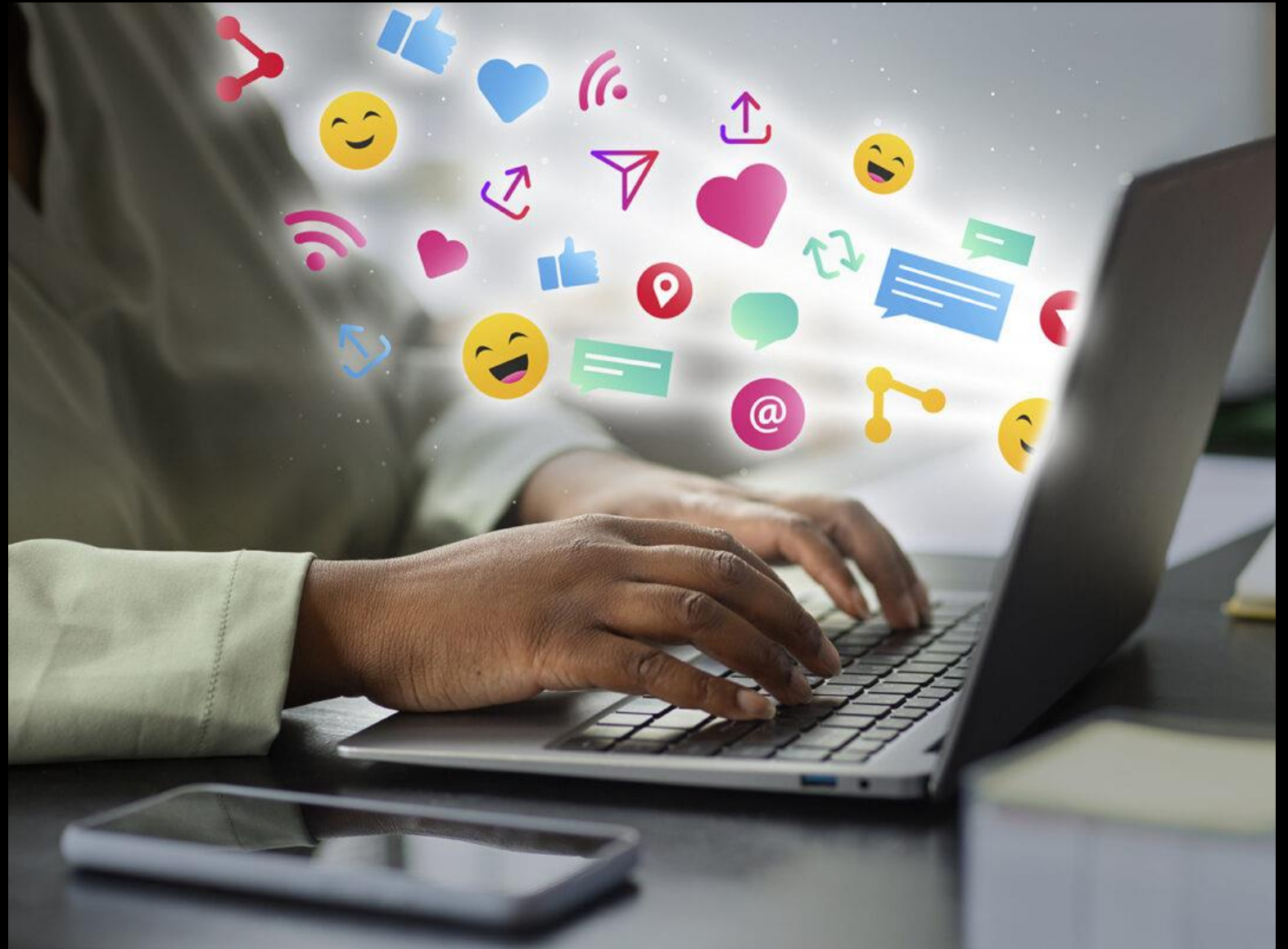
2nd Result for Organic Search

Even top search results can be manipulated for fake sites



Social Media Scams

- There are a lot of fake profiles on social media. Another possibility is that it's a fake account that will attempt to scam you later on and has the same name and photo as one of your actual friends.



QR Code Scams

- **Who thought that a QR code would be harmful?**
- **They are commonplace, particularly at restaurants. Hackers have the ability to cover the official sticker with their own. in order for you to be taken to a fake website when you scan it.**



Vishing Scams

- One kind of phishing attack done over the phone is called "voice phishing," or "vishing."
- Scammers are able to imitate phone numbers that look just like well-known numbers, such as your bank's.

What is Vishing?



Silly name. Serious threat. Don't be caught off guard.

What Protects You Against Phishing Attempts?



Call and verify! - Verify that you are talking to the correct person



Check the address - Always check the email address and URL for spelling mistakes



Enable Multi-Factor Authentication

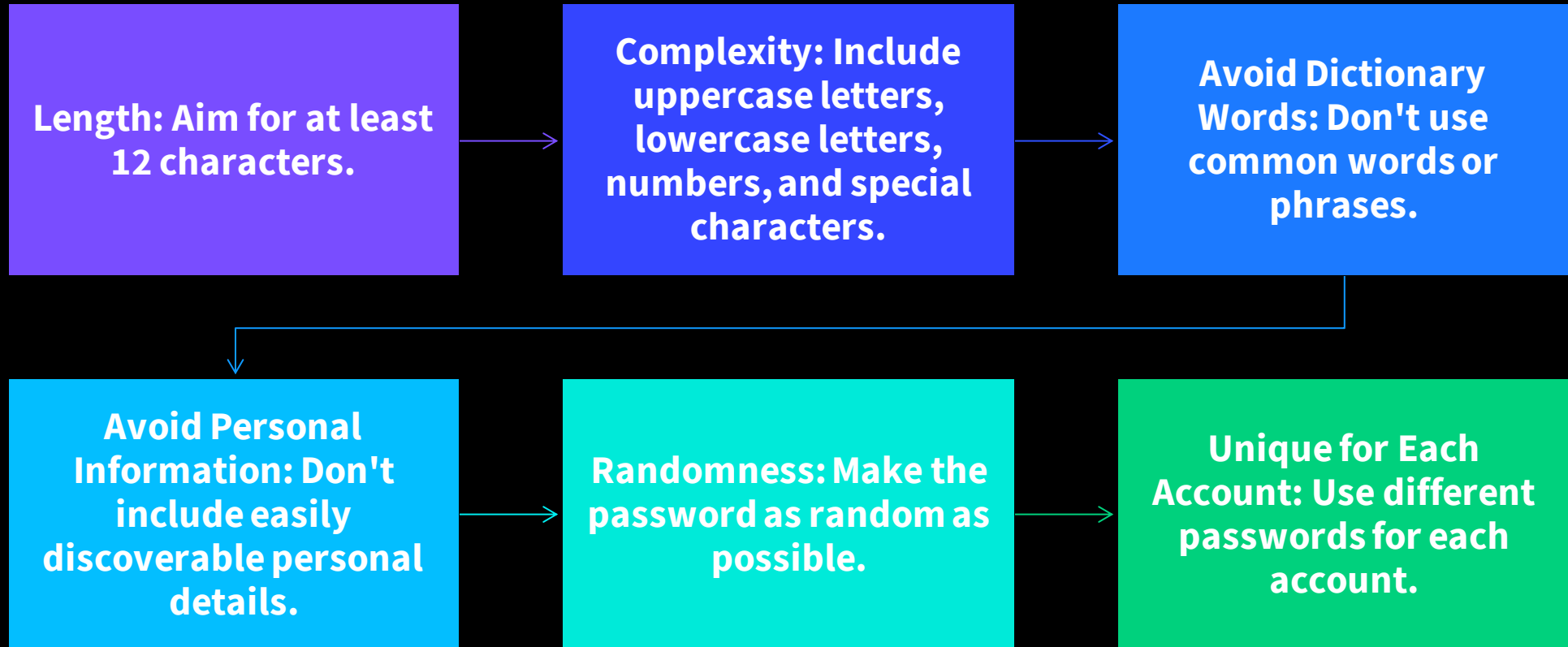


Take note of the message's style.

7 characters	1 minute
8 characters	1 hour
9 characters	3-4 days
10 characters	7 months
11 characters	40 year
12 characters	2000 years

*How long will it
take
to crack your
password*

How to create strong password:



HOWEVER

01

Indian enterprises and government organizations encountered 5 billion cyberattacks in 2023.

02

There was an average quarterly increase of 63% in cyberattacks throughout the year.

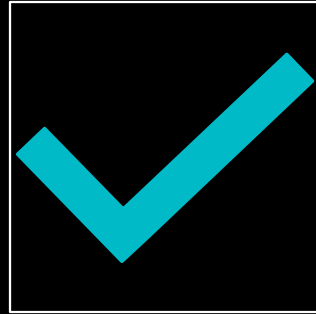
03

So even if you have a **STRONG PASSWORD**, it may still not be enough

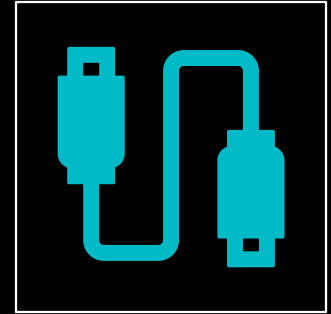
What type of Multi-Factor Authentication to use?



Most common is text based (SMS), but
it's the least secure



It's better to use authenticator apps like
Google or Microsoft Authenticator



Or even better yet, a physical USB key

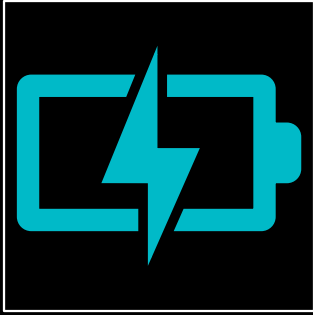
And that is why

... You should enable Multi-Factor Authentication

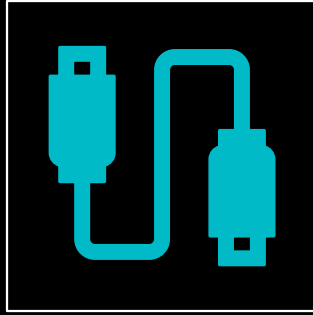
This will help to **protect your account** if your password was stolen or leaked in a data breach.



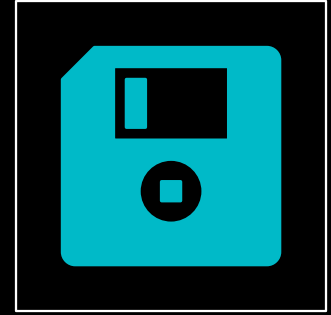
How to use USB Safely



Avoid public charging stations. They may be compromised.



Don't plug any USB that isn't yours into your device

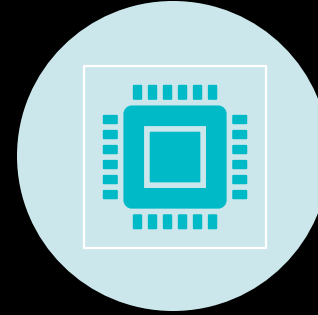


Encrypt the data on the USB device in case you lose it or it gets stolen.

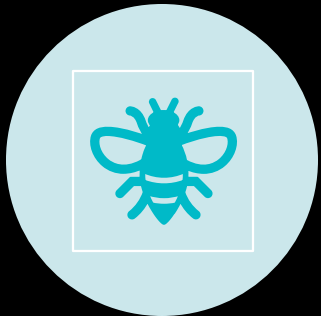
Responding to cyber security:



National cyber crime
reporting portal
: <https://cybercrime.gov.in/>



Botnet cleaning and
malware analysis
: <https://www.csk.gov.in/>



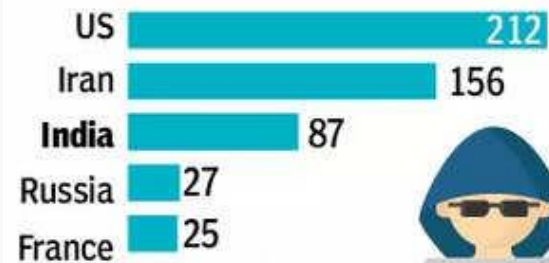
Twitter handle :
@Cyberdost



Helpline : 1930

1 OUT OF 5 PEOPLE AFFECTED GLOBALLY: STUDY

Countries with most data breaches



Source:
Surfshark

No. of breached
accounts in mn



➤ Till Nov, nearly 953 million accounts were breached against 922 million in the same period last year

➤ Some of the biggest data breaches this year included COMB, Clubhouse, Facebook and Raychat

TOI

FOR MORE INFOGRAPHICS DOWNLOAD TIMES OF INDIA APP

Available on the
App Store

Google play

Windows
Phone

Indian enterprises and government organizations encountered 5 billion cyberattacks in 2023. There was an average quarterly increase of 63% in cyberattacks throughout the year. So even if you have a STRONG PASSWORD, it may still not be enough. You can check if yours was leaked at haveibeenpwned.com



Thank you
