APPS BY VIKAS

Meet Vikas



GenzLudo

Ludo with 3D characters and up to 8 players. A first-of-its-kind no-teaming-up feature keeps play fair. Try it - you'll love the difference.

Download on Google Play



Kachu

Too much scrolling straining your neck? Add your addictive apps and complete daily neck exercises to unlock them.

Download on Google Play

Homograph Attack

A simple 5-minute guide to spotting fake look-alike links and protecting your accounts.

What is it?

A homograph attack happens when a scammer creates a fake domain using letters that look like normal English letters. The fake link may look real to your eyes, but it is a different website.

LOOKS REAL	FAKE VISUAL EXAMPLE
apple.com	apple.com
First letter: English a (U+0061)	First letter: Cyrillic a (U+0430)

Important: the fake domain above is only a visual example. Do not search for or open it.

How the attack works

1. The attacker registers a look-alike domain.
2. They copy the design of a trusted login page.
3. You receive the link by email, message, comment or advertisement.
4. You enter your email, password, OTP or payment details.
5. The information goes to the attacker, not the real company.

Possible result: stolen passwords, account takeover, payment fraud, fake downloads or malware.

How to protect yourself

Use layers of protection. No browser or extension can stop every fake link.

1	Do not log in from a message link Open the official app or type the known website address yourself.
2	Check the real domain Read the main domain carefully. A trusted name inside a long subdomain does not make the site genuine.
3	Watch for xn-- Browsers may show suspicious international domains as Punycode beginning with xn--. Treat it as a warning and verify the site.
4	Use a password manager It normally fills a saved password only on the exact domain. If it does not autofill, stop and check.
5	Turn on phishing protection Keep Chrome Safe Browsing or Safari's Fraudulent Website Warning enabled.
6	Use 2-step verification Prefer a passkey or authenticator app. This reduces damage if a password is stolen.
7	Do not trust the padlock alone HTTPS encrypts the connection, but a fake website can also have HTTPS.

Free tools and official guides

Platform	Recommended option	Link
Chrome / Edge / Brave	TypoProtect - optional, free and open source	Install
Source code	Review TypoProtect's public code	GitHub
Chrome	How Chrome displays suspicious IDN links	Official guide
Safari	Enable Fraudulent Website Warning	Apple guide
Any browser	Check a URL with Google Safe Browsing	Check URL

Best quick rule: if a login link arrives unexpectedly, do not use it. Open the official app or type the website address yourself.

Note: TypoProtect is a third-party extension, not an official Google product. Browser warnings and extensions add protection, but they are not a guarantee.

More things worth exploring

Find more free guides at vikasbuilds.com/resources