Ghost Pairing

Prelims: *Current events of national and international importance*

Why in News?

The Indian Computer Emergency Response Team (CERT-In) has issued an advisory about an active threat campaign targeting WhatsApp users with a new technique called Ghost pairing.

- It is one of the ***new phone hacking techniques,*** where threat actors use social engineering and messenger apps such as WhatsApp and Telegram.
- WhatsApp ghost pairing uses the “Linked Devices” feature.
- **Process -** A scammer tricks a user into sharing a verification code or scanning a QR code, mostly through fake messages pretending to be support or known contacts.
- Once linked, the attacker’s device silently syncs with the victim’s WhatsApp.
- The victim continues chatting as usual, unaware that messages, media, and sometimes even contacts are being mirrored in some other unwanted device.
- They initially build trust by having the name of a known contact (in the potential victim's phone list), or a government agency representative (Income Tax), or a bank executive.
- They send a message with a 'Hi, check this photo'.
- The message contains a link with a Facebook-style preview, which later leads to a verification process via phone number.
- As part of a social engineering tactic, the threat actors use urgency or panic-inducing statements, such as if the user don't perform this action, their bank account will be frozen, or the phone number will be blocked immediately.
- Many users rarely check their linked devices, allowing attackers prolonged access.
- Since the pairing uses a legitimate WhatsApp feature, victims often realise something is wrong only after data misuse, fraud, or leaked private

conversations.

- Scammers depend mostly on human psychology, posting situations of utmost urgency.
- **Prevention -** Prevention starts with just being aware. Never share WhatsApp verification codes or scan QR codes sent by others.
- Regularly check the “Linked Devices” section and remove devices that might look fishy and problematic.
- Enable two-step verification for increased protection.
- Most importantly, it is necessary to rethink when messages create panic or urgency.
- A few seconds of verification and cross-checking can prevent weeks of damage and loss of privacy.

Reference

Deccan Herald | Ghost Pairing

