Smartphone Security Advice

Ahmadiyya Muslim Community UK IT Committee

In light of recent security incidents targeting members of our organisation, we find it crucial to draw your attention to a type of cyber-attack called **"SIM Swapping"** as well as other prevalent mobile security threats and scams. Your awareness and proactive steps can prevent potential security breaches and safeguard both personal and Jama'at data. Some of the attacks and prevention methods are listed in this note below, however we strongly advise you to read the advice provided on the following website:

https://us.norton.com/blog/online-scams/whatsapp-scams

Common Attacks & Prevention

1. SIM Swapping Attack

How It Works: The attacker convinces the victim to share a code that they will receive via SMS. This code is the two-factor authentication (2FA) code that WhatsApp uses to verify the identity of a user trying to set up the app on a new device. Once the attacker has the 2FA code, they can complete the setup of the victim's WhatsApp on their device, effectively taking over the account.

Prevention:

- Never share your 2FA codes with anyone.
- Use app-based 2FA like Microsoft Authenticator or Google Authenticator where possible, as they are more secure than SMS-based 2FA.

2. Phishing Scams on Mobile

How It Works: Attackers send deceptive messages via SMS, WhatsApp, or other platforms with malicious links or requests for personal data.

Prevention:

- Don't click on unfamiliar or suspicious looking links.
- Confirm the identity of anyone asking for sensitive information.
- **DO NOT** share or send any personal data or Jamat data to people or organisations that you are not familiar with. If in doubt, please contact: security@ahmadiyyauk.org in the first instance.

3. Malicious Mobile Apps

How It Works: Some apps, especially those from third-party stores, may contain malware (i.e. harmful viruses).

Prevention:

- Only download apps from official stores (Google Play, Apple App Store).
- Regularly update your apps and phone operating system.

4. Wi-Fi Eavesdropping

How It Works: When connected to unsecured public Wi-Fi networks, attackers can intercept data transfers.

Prevention:

- Avoid public Wi-Fi for sensitive activities.
- Use a personal VPN (Virtual Private Network) when accessing organisational resources.

5. Prevent unknown users from adding you to WhatsApp groups

There is a setting that you can tweak in the privacy section of you WhatsApp account that spares you from getting added to random groups.

This setting lets you customise who can add you to groups and, by default, the setting is set to 'Everyone', which means anyone with your phone number can add you in a group. It is important to note that group admins can send you invite links and nudge you to join groups, even after you tweak the settings.

In order to avoid getting added to groups by random people, follow the steps below:

1. Open **WhatsApp**, click on the **three dots** on the top right corner of the screen.
2. Click on the **Settings** option and then tap **Account**.
3. Click on **Privacy** > **Groups**. The default setting is likely to be set to '**Everyone**'.
4. You can select from three options — **'Everyone', 'My Contacts'**, and '**My Contacts Except'.**
5. The 'Everyone' option lets any user with your phone number add you in a group without your permission.
6. The 'My Contact' option only lets those users add you in groups whose numbers you have saved in your contact list.
7. The last 'My Contacts Except' option lets you choose exactly who can add you to groups by letting you filter further and delist the contacts you don't want to be added by to a group.

General Best Practices:

1. Set up two-step verification on your accounts.
2. Regularly review the security settings on your accounts.
3. Keep your mobile device software updated.
4. Be cautious about granting applications unnecessary permissions.
5. Always have a secure backup of essential data.

We believe that some members of the Jamaat have had their phones hacked and data may have been stolen. If you believe you've been targeted or compromised and are asked to pay money (also known as a ransom payment), then **Do not pay any money EVEN if the message looks to be from someone you know.** Instead, contact the IT Security team immediately and we will advise you further:

security@ahmadiyyauk.org

Please share this memo with your teams, and let's prioritise digital safety at all levels of our operations.