**Threat Notification: SIM Swapping Attacks**

**Title**

SIM Swapping: A Rising Threat to Mobile Security and Two-Factor Authentication

**Summary**

SIM swapping is a sophisticated attack where criminals manipulate mobile carriers to transfer a victim's phone number to a SIM card under their control. This allows attackers to intercept SMS-based two-factor authentication codes, potentially leading to unauthorized access to various accounts, including financial and social media platforms.

**Details**

SIM swapping attacks typically follow these steps:

1. Attackers gather personal information about the target through social engineering or data breaches.
2. They contact the victim's mobile carrier, impersonating the account holder.
3. Using social engineering tactics, they convince the carrier to transfer the phone number to a new SIM card.
4. With control of the phone number, attackers can intercept SMS-based 2FA codes and reset passwords for various accounts.

**Risk**

The risk associated with SIM swapping is high due to its potential for significant financial loss, identity theft, and unauthorized access to sensitive information. Specific risks include:

* Cryptocurrency theft from digital wallets
* Unauthorized access to bank accounts and financial services
* Hijacking of social media and email accounts
* Corporate espionage through access to business accounts and sensitive information
* Reputational damage, especially for high-profile individuals

**Detection**

Signs of a potential SIM swap attack include:

* Sudden loss of cellular service
* Inability to send or receive text messages or make calls
* Unexpected notifications about SIM card or phone number changes
* Unusual activity on social media or financial accounts
* Inability to access online accounts

**Prevention**

To protect against SIM swapping attacks:

1. Use non-SMS based two-factor authentication methods (e.g., authenticator apps, hardware tokens)
2. Set up strong, unique passwords for all accounts
3. Limit personal information shared on social media
4. Contact your mobile carrier to set up additional security measures (e.g., PIN or passphrase for account changes)
5. Regularly monitor account activity for any suspicious behavior

**Response**

If you suspect you're a victim of a SIM swap attack:

1. Contact your mobile carrier immediately to regain control of your phone number
2. Change passwords for all important accounts, especially financial and email
3. Review recent account activity for any unauthorized transactions
4. Consider freezing your credit to prevent potential identity theft
5. Report the incident to local law enforcement and relevant financial institutions

**Conclusion**

SIM swapping poses a significant threat to mobile security and the integrity of SMS-based two-factor authentication. By understanding the risks and implementing strong security measures, individuals and organizations can better protect themselves against this evolving cyber threat.