How to Protect against Iranian Targeting of Accounts Associated with National Political Organizations

IRANIAN SPEARPHISHING ACTIVITY

The Cybersecurity and Infrastructure Security Agency (CISA) and Federal Bureau of Investigation (FBI) have observed actors affiliated with the Iranian Government's Islamic Revolutionary Guard Corps (IRGC) targeting and compromising the personal and business email accounts of Americans, probably to stoke discord and undermine confidence in U.S. democratic institutions. Specifically, IRGC cyber actors are targeting individuals associated with national political organizations and campaigns, as well as individuals who have worked on issues related to Iranian and Middle Eastern affairs. This includes current and former senior government officials, think tank personnel, journalists, activists, and lobbyists. IRGC actors seek access to American personal and business accounts using social engineering techniques that target email and chat applications. The actors impersonate personal or professional contacts of potential victims in an attempt to direct them to a spoofed, or convincing but fake, email login page. This page then prompts victims to enter login credentials, which the cyber actors then use to access the victim's accounts. Observed techniques by these actors include impersonation of known individuals, requests for interviews, invites for speaking engagements and high-profile events, and solicitations from U.S. political campaigns. Although we have not seen this actor do so, some nation-state actors use generative artificial intelligence capabilities to increase the believability of social engineering efforts.

This fact sheet provides steps that individuals and organizations can take to enhance their security and resilience to protect against this activity. CISA and FBI strongly recommend all potential victims apply the mitigations detailed in this fact sheet, including protecting their personal and business accounts with phishing-resistant multifactor authentication (MFA). MFA that uses SMS- or email-based authenticators is not sufficient to protect against the specific tactics these actors are employing.

For additional information on Iranian state-sponsored malicious cyber activity, see CISA's Iran Cyber Threat Overview and Advisories webpage and the FBI's Iran Threat webpage. For additional tactics, techniques, and procedures affiliated with this identified IRGC cyber activity to include mitigation options, see FBI advisory "Iranian Cyber Actors Targeting Personal Accounts to Support Operations"and US Department of Justice Press Release "Three IRGC Cyber Actors Indicted for 'Hack-and-Leak' Operation Designed to Influence the 2024 U.S. Presidential Election."

MITIGATION STRATEGIES

Individuals

The below steps are ways to protect against phishing techniques. While all individuals should follow these practices, CISA and FBI highly recommend that those specifically identified as target groups remain vigilant.

To spot and identify possible social engineering attempts, watch out for:

- **Unsolicited contact** from individuals you either do not know personally or individuals you know but claim to be using a new account or phone number.
- **Unusual email requests** from known individuals.
- **Accounts attempting to pass links or files via social media**, especially coming from people you do not know or individuals who do not typically share files in that manner.
- **Email messages conveying suspicious alerts** for online accounts. Never access accounts via email links but instead login directly via the website.
- **Unsolicited email messages containing shortened links** (e.g., tinyurl, bit.ly).

To help mitigate or prevent successful phishing attempts, apply the following best practices, many of which may be found at Project Upskill, a series of guides for non-technical, high-risk users.

- **Use phishing-resistant MFA for email, social media and collaboration tools accounts** [Project Upskill, Module 2, Topic 2.2].
- **Use a password manager to generate strong, unique passwords for all accounts** [Project Upskill, Module 2, Topic 2.0, Topic 2.1].
- **Do not access links in emails, chat messages, or social media account alerts.** Go to the site directly to verify the legitimacy of the alert.
- **Keep applications and OSs updated** [Project Upskill, Module 1, Topic 1.1].
  - Install updates promptly to prevent exploitation of vulnerabilities by threat actors.
  - Enable automatic OS and app updates for proactive security maintenance.
- **Ensure your device's native antivirus and anti-malware protections are enabled** to protect against the latest malware threats [Project Upskill, Module 1, Topic 1.2].

Organizations

Organizations can help prevent or mitigate the effects of an incident by applying the following:

- **Require phishing-resistant MFA** for all employees. Phishing-resistant MFA (i.e., physical security key or passkey) offers the greatest level of protection.
- **Offer an enterprise password manager** to employees, enabling the random generation of unique passwords for each account. Password managers help protect against phishing attacks by only filling passwords on valid websites, providing a valuable indication of potential anomalies or security risks.
- **Enable anti-phishing and anti-spoofing security features** supplied by email service providers that automatically block malicious emails.
- **Train staff to only use official accounts for business, never personal accounts**. Official accounts will typically have greater protections and security measures enabled than personal accounts.
- **Train staff to confirm unusual or suspicious emails or messages from known or unknown contacts** through a communication method separate from the one impacted by the unusual or suspicious outreach to verify its authenticity.
- **Strongly recommend employees routinely update the software on their personal devices** and turn on MFA for their personal accounts.
- **Add an email banner to messages coming from outside your organization**.
- **Enable alerts for suspicious activity**, such as foreign IP address logins.

RESOURCES

- See Joint Phishing Guidance: Stopping the Attack Cycle at Phase One for common phishing techniques and guidance for network defenders of all organizations.
- Project Upskill is a series of guides for non-technical, high-risk users.
- Election and campaign infrastructure stakeholders and the public can find additional resources about how to protect against cyber and physical threats at #Protect2024.

INCIDENT REPORTING INFORMATION

If you observe suspicious activity similar to the examples listed above, contact your local FBI office or the FBI's 24/7 Cyber Watch (CyWatch) at (855) 292–3937 or by email at CyWatch@fbi.gov. Field office contacts can be identified at fbi.gov/contact-us/field. Cyber incidents impacting election and campaign infrastructure can also be reported to CISA by calling 1-844-Say-CISA (1-844-729-2472), emailing report@cisa.dhs.gov, or reporting online at cisa.gov/report.