IT Security Supply Chain OT Security Insider Threat Physical Security Interoperable Communications

CISA INSIGHTS

DEFEND TODAY, SECURE TOMORROW

# ACTIONS TO COUNTER EMAIL-BASED ATTACKS ON ELECTION-RELATED ENTITIES

*SEPTEMBER 10, 2020*

## THE THREAT AND HOW TO THINK ABOUT IT

Malicious cyber actors have been known to use sophisticated phishing operations to target political parties and campaigns, think tanks, civic organizations, and associated individuals. Email systems are the preferred vector for initiating malicious cyber operations. Recent reporting shows 32 percent of breaches involve phishing attacks, and 78 percent of cyber-espionage incidents are enabled by phishing.[1,2]

Cyber actors launching phishing attacks often seek to entice users to do one of three things.

- Click on a link and turn over credentials (username and password), so the cyber actor can gain access to an account.
- Open an attachment or click a link that delivers the cyber actor's malware.
- Click a link to a website that the cyber actor monitors; this verifies that the email account is valid for subsequent targeting.

Cyber actors can also use credential-based techniques to gain access to accounts in various ways.

- Password spraying attacks rely on cyber attackers using a commonly used password against multiple usernames.
- Brute-force attacks rely on cyber attackers knowing the username and attempting several passwords.
- Credential stuffing attacks rely on cyber attackers using usernames and password combinations gained from data breaches against other accounts.

To protect against these attacks, the Cybersecurity and Infrastructure Security Agency (CISA) strongly recommends organizations involved in any election-related activities prioritize the protection of accounts from email-based attacks by:

- Using provider-offered protections, if utilizing cloud email.
- Securing user accounts on high value services.
- Implementing email authentication and other best practices.
- Securing email gateway capabilities.

## WHEN USING CLOUD EMAIL, USE PROVIDER-OFFERED PROTECTIONS

Organizations that use cloud email providers should enable various protections their provider offers.

a. Require multi-factor authentication (MFA) for all user email accounts.

- Use either physical security keys (such as those following the FIDO2 standard) or authentication apps (such as those following the TOTP algorithm).
    - Physical security keys offer protection against phishing attacks by working as a second, physical factor of authentication and only authenticating when a user is on the correct

[1] Verizon 2019 Data Breach Investigation Report, https://enterprise.verizon.com/resources/reports/dbir/

[2] Joint CISA/National Cyber Security Centre (NCSC) Alert (AA20-099A): COVID-19 Exploited by Malicious Cyber Actors, https://www.us-cert.gov/ncas/alerts/aa20-099a

website. Thus, even if a user is tricked into supplying their password to a phishing website, the physical security key will still block attackers from accessing their account.

- Authentication apps work by having a user enter a code from an app. Although authentication apps can still be vulnerable to phishing attacks, they offer more protection than SMS or email-based MFA.

➢ Only use SMS and email-based MFA methods if other forms of MFA are unavailable. SMS and email-based MFA methods are vulnerable to phishing and SIM swap attacks, though they still offer better protection than password-based single-factor authentication.

b. When available, enroll user accounts in advanced protection services.

➢ These services provide the highest level of protection against phishing and other attacks, applying robust filtering techniques, with many requiring physical security keys. For instance, Google offers an Advanced Protection service for all users, and Microsoft offers an Advanced Threat Protection service. Google also offers an Enhanced Account Protection service at no cost to at-risk election-related organizations. *Note: CISA includes these references with the intention of highlighting the types of services available; doing so does not constitute endorsement of any particular company or service.*

## SECURE USER ACCOUNTS ON HIGH-VALUE SERVICES

Protect individual accounts on high-value services to mitigate the impact of a successful phishing attack.

a. Enroll in a password manager service for your organization and encourage employees to use it.

➢ Password managers protect against phishing by generating secure, random passwords and automatically filling passwords when visiting websites. Password managers will not automatically enter passwords on malicious websites, giving employees a crucial cue that they should not proceed.

b. Require MFA for user accounts on all high-value services when possible.

➢ If possible, deploy physical security keys for access to high-value services.

➢ After physical keys, authentication app-based MFA (TOTP) is the next safest option, followed by SMS and email-based MFA. Use SMS and email-based MFA only when no other MFA options are available.

➢ If a high-value service does not support any form of MFA, consider switching to a similar service that does offer MFA.

c. Eliminate unnecessary password composition and rotation requirements in favor of secure, human-friendly requirements.

➢ Recent research shows that excessive password requirements (such as including special characters or numbers) tend to cause user frustration and may reduce security.[3] Consider adopting password requirements to match guidance from the National Institute of Standards and Technology (NIST) in Special Publication 800-63B, which recommends long, human-friendly, memorable passwords (e.g., sequences of several words).

d. Consider registering your organization for a password breach monitoring service.

➢ Password reuse is a leading cause of account compromise. Attackers often use breached credentials to attempt to access other services for which the victim may have reused credentials. In addition to encouraging use of password managers to reduce password reuse, organizations should consider monitoring password breaches for exposed employee credentials. Several vendors offer password breach monitoring services and will send notifications to an organization if employee passwords appear in a data breach.

[3] NIST Special Publication 800-63B, https://pages.nist.gov/800-63-3/sp800-63b.html

## IMPLEMENT EMAIL AUTHENTICATION AND OTHER BEST PRACTICES

Implement email authentication and other best practices to reduce attackers' ability to send spoofed phishing emails originating from your organization. For additional guidance, refer to CISA Binding Operational Directive (BOD) 18-01.

a. Enable STARTTLS.
   - ➢ When enabled by a receiving mail server, STARTTLS signals to a sending mail server that the capability to encrypt an email in transit is present. While it does not force the use of encryption, enabling STARTTLS makes on-path attacks more difficult.

b. Disable outdated protocols and ciphers.
   - ➢ Ensure that outdated, insecure protocols—such as SSLv2 and SSLv3—as well as 3DES and RC4 ciphers are disabled on mailing servers.

c. Implement SPF and DKIM.[4]
   - ➢ SPF and DKIM allow a sending domain to effectively "watermark" their emails, making unauthorized emails (e.g., spam, phishing email) easy to detect.

d. Configure a DMARC policy of "reject", if possible, or at minimum, "p=none".[5]
   - ➢ When an email is received that does not pass an organization's posted SPF/DKIM rules, DMARC tells the recipient what the domain owner would like done with the message.
   - ➢ Setting a DMARC policy of "reject" provides the strongest protection against spoofed email, ensuring that unauthenticated messages are rejected at the mail server, even before delivery. Additionally, DMARC reports provide a mechanism for an organization to be made aware of the source of an apparent forgery—information that they would not normally receive otherwise. Multiple recipients can be defined for the receipt of DMARC reports.

## SECURE EMAIL GATEWAY CAPABILITIES

Organizations operating their own email gateways should secure email gateways, appliances, and services to intercept phishing emails.

a. Deploy an email filter solution that screens based on headers and malicious content (e.g., infected attachments), categorizes email, inspects Uniform Resource Locators (URLs) against reputation feeds, and has customizable rule-based filters.

b. Strip and/or block emails containing active content (e.g., ActiveX, Java, Visual Basic for Applications [VBA]), or macros) by default. Administrators should allowlist such content only for legitimate reasons.

c. Consider reformatting hyperlinks in the body of email messages by rewriting URLs as plaintext.

d. Deploy sandboxing or detonation chambers to safely isolate malicious links.

e. Ensure detection signatures and blocklists are up to date.

f. Block email beyond a certain size and/or containing attachments that exceed a certain size.
   - ➢ Consider legitimate needs to receive large file sizes and limit file size to suit organizational need.

g. Block certain file extensions—including unknown or unused attachments that should not typically be transmitted over email—to prevent vectors such as .scr, .exe, .pif, and .cpl.

[4] See CISA Binding Operational Directive 18-01, https://cyber.dhs.gov/bod/18-01/#spf--dkim

[5] See CISA Binding Operational Directive 18-01, https://cyber.dhs.gov/bod/18-01/#dmarc

- ➢ To the extent feasible, filter out mislabeled file extensions, for example, an executable (.exe) file labeled as a document (.doc) file.

h. Open and analyze compressed and encrypted formats, such as .zip and .rar, that attackers may use to conceal malicious attachments in obfuscated files or information. If unable to open and analyze such content, consider blocking encrypted .zip and other files. However, blocking attachments might keep legitimate files from reaching recipients, which may hinder business functions. Consider using workarounds, such as allowlisting (e.g., trusted senders), to limit negative impacts to operations.

- ➢ Consider removing the encrypted content from the message and putting it in an out-of-band delivery solution (e.g., web-based portal), replacing the content with a token/link in the original message.

i. Ensure all email gateways, appliances, or services are configured to use only approved Domain Name System (DNS) resolvers and forwarders.

j. Consider implementing warning banners to alert users about emails (particularly those with links and attachments) that originate from outside the organization (place trusted domains on your allowlist to reduce unnecessary implementation).