Security For IT Admins/Developers

SUMMARY:

This webinar is designed to empower end users with practical knowledge and tools to protect their accounts and email communications. It covers essential topics such as configuring Multi-Factor Authentication (MFA), identifying phishing and malicious emails, reporting suspicious emails, blocking unwanted senders or domains, and understanding common attack methods that can compromise accounts. By the end of the session, users will be equipped with actionable steps to enhance their personal and organizational security.

KEY POINTS:

- **Understanding Common Account Attacks -** Gain awareness of different types of attacks, such as phishing, brute force, and credential stuffing, that can compromise your accounts. Learn how to stay vigilant and adopt best practices to safeguard your credentials and personal information.
- **How to Configure MFA -** Learn how to set up Multi-Factor Authentication (MFA) to add an extra layer of security to your accounts. MFA requires a second form of verification (e.g., a code sent to your phone) in addition to your password, significantly reducing the risk of unauthorized access.
- **Identifying Phishing and Malicious Emails -** Discover how to recognize phishing emails and malicious content by checking for suspicious sender addresses, unexpected attachments, and urgent or too-good-to-be-true requests. This skill helps prevent falling victim to scams or malware.

TARGET AUDIENCE

- End-Users