

Avoiding M365 Smishing: 3 Real-Life **Examples** and **Solutions**

Fake Account Verification

What Happens:

A user receives a text message claiming to be from Microsoft 365 Support, warning of suspicious activity on their account. The message instructs them to click a link to verify their account information or risk being locked out.

How to Identify and Avoid:

- Verify the sender's phone number and check for any suspicious or unfamiliar numbers.
- Look for grammatical errors or unusual language that might indicate a phishing attempt.
- Do not click on any links in the text message. Instead, go directly to the official Microsoft 365 login page and check for any security notifications.



Urgent Password Reset Request

What Happens:

A text message alerts the user that their Microsoft 365 password has been compromised and urges immediate reset via a provided link. The message creates a sense of urgency to prompt a quick response.

How to Identify and Avoid:

- Be cautious of urgent requests for personal information or password changes.
- Check the URL of the provided link; official Microsoft links will usually be part of the microsoft.com domain.
- Contact your IT department or Microsoft Support directly if you are unsure about the legitimacy of the message.



365 Subscription Renewal

What Happens:

The user receives a text message claiming their Office 365 subscription is about to expire, with a link to renew it. The link leads to a fake page designed to steal credit card information.

How to Identify and Avoid:

- Verify your subscription status through the official Microsoft 365 portal or your subscription manager.
- Be wary of messages that ask for payment or sensitive financial information via text.
- Report the message to Microsoft and your IT department.



Utilise **Microsoft Intune** for Mobile Phone Management

Microsoft Intune is a cloud-based service that helps manage and secure mobile devices. By using Intune, you can implement robust security measures to protect against smishing attacks.

Key features include:

- Device Compliance Policies
- App Protection Policies
- Conditional Access
- Threat Protection Integration
- Automated Remediation
- User Education and Awareness

By incorporating **Microsoft Intune** into your mobile phone management strategy, you can establish a comprehensive security framework that effectively protects your business against smishing and other mobile threats.

Contact us to learn more!