Operational Guide:

Anti-Phishing in Microsoft 365

1 CardinalByte Expert Insight

Over 90% of data breaches begin with a phishing email. Microsoft 365 has powerful built-in protections, but they are often disabled by default. Turning on ”First Contact Safety Tips” and ”Impersonation Protection” can stop a breach before it happens.

2 Why It Is Required

The IRS Security Six mandates Anti-Phishing software. For tax professionals, phishing isn’t just about viruses; it’s about stealing the credentials to your tax software.

3 Regulatory Body

IRS and **FTC**.

4 How to Implement

Access the Microsoft Defender for Office 365 portal and configure ”Anti-Phishing” policies that look for domain spoofing and user impersonation.

5 Step by Step Instructions

1. **Portal Access:** Go to security.microsoft.com.
2. **Policies:** Navigate to Email & Collaboration -> Policies & Rules -> Threat Policies.
3. **Anti-Phishing:** Click on the Default Policy.
4. **Enable Impersonation:** Add your high-profile employees (Partners/Owners) to the impersonation protection list.
5. **Safety Tips:** Enable the ”Show first contact safety tip” to warn users when they get an email from a new sender.

6 Tactical and Operational Checklist

- ☐ SPF, DKIM, and DMARC records configured for your domain.
- ☐ Impersonation protection active for all key staff.
- ☐ ”First Contact” banners visible in Outlook.
- ☐ External email tagging (adds [EXTERNAL] to subject lines) enabled.

7 Expert Tip

Enable ”External Email Tagging.” It forces your staff to pause when they see a ”CEO Request” that actually originated from an external Gmail address.