Cyber Security Checklist: Microsoft 365 & Outlook Protection

Voice Phishing (Vishing)

- ☐ Verify callers using official contact information from the organization website.
- ☐ Never share passwords, Multi-Factor Authentication (MFA) codes, banking information, or Social Security numbers over the phone.
- ☐ Be suspicious of urgent requests involving payroll changes, gift cards, wire transfers, account verification, or password resets.
- ☐ Report suspicious calls to the Technology Department and the FTC at reportfraud.ftc.gov.

Microsoft Outlook Email Safety

- ☐ Use separate personal and work/school email accounts.
- ☐ Be cautious with email attachments, links, and QR codes, even when messages appear to come from someone you know.
- ☐ Verify unexpected requests through a phone call, Microsoft Teams chat, or another trusted communication method.
- ☐ Use Outlook's Report Phishing or Report Junk button for suspicious messages. Also report using CyberNut.
- ☐ Do not click Unsubscribe in suspicious or unexpected emails.
- ☐ Type website addresses directly into your browser instead of clicking links in emails.
- ☐ Hover over links to verify the destination before clicking.
- ☐ Be cautious when using Reply All, Forwarding, and BCC.
- ☐ Watch for external sender warnings and unusual sender addresses.
- ☐ Never assume an email is safe simply because it appears to come from a coworker or administrator.

Microsoft 365 Account Security

- ☐ Use a strong, unique password for your Microsoft 365 account.
- ☐ Enable and use Multi-Factor Authentication (MFA).
- ☐ Never share your password or MFA approval codes with anyone, including Technology staff.
- ☐ Review unexpected MFA prompts carefully. If you did not initiate the login, deny the request and report it immediately.
- ☐ Lock your computer whenever you leave your workspace (Windows + L).
- ☐ Keep Windows, Microsoft Edge, Microsoft Office, and browsers updated.
- ☐ Sign out of Microsoft 365 applications when using shared or public devices.
- ☐ Store work files in approved district locations such as OneDrive and Teams.
- ☐ Never enter credentials into pop-up windows or pages reached through unsolicited email links.

Signs of Phishing

☐ Use generic greetings such as Dear User or Dear Customer.

☐ Create urgency, fear, or pressure to act immediately.

☐ Request passwords, MFA codes, financial information, or personal data.

☐ Claim your account will be disabled unless you take immediate action.

☐ Include unexpected invoices, payment requests, or gift card purchases.

☐ Contain QR codes requiring you to log in or verify your account.

☐ Use shortened or disguised links.

☐ Contain poor grammar, spelling errors, or unusual formatting.

☐ Come from addresses that do not match the organization they claim to represent.

Warning Signs of a Compromised Microsoft 365 Account

☐ People report receiving emails or Teams messages you did not send.

☐ You receive MFA prompts that you did not initiate.

☐ Your mailbox contains unfamiliar emails in Sent Items.

☐ Email forwarding rules were created without your knowledge.

☐ Your email signature, inbox rules, or account settings have changed unexpectedly.

☐ Your password no longer works.

☐ Your account recovery information has changed.

If You Suspect a Compromise

☐ Contact the Technology Department immediately.

☐ Change your Microsoft 365 password.

☐ Review MFA settings and remove unknown devices.

☐ Check Outlook inbox rules, forwarding settings, and email signatures.

☐ Review recent account activity for suspicious logins.

☐ Warn coworkers not to respond to suspicious messages sent from your account.