🧼 Employee Cyber Hygiene Starter Guide

A simple, one-page guide to help your team build strong cybersecurity habits.

✅ Daily Habits

- • Use strong, unique passwords for each system or account.
- • Lock your computer when stepping away—even for a minute.
- • Think before you click: be cautious with links and attachments.
- • Use only company-approved tools for communication and file sharing.
- • Report anything suspicious right away—even if you're not sure.

🚩 Phishing Red Flags

- • Emails with urgent requests, especially involving money or passwords.
- • Misspelled email addresses or suspicious links.
- • Unexpected attachments or login requests.
- • Emails asking you to confirm account info or payment methods.

🛡️ Best Practices

- • Enable multifactor authentication (MFA) wherever possible.
- • Keep software and devices updated—don't delay patches.
- • Never share your password, even with coworkers.
- • Only access company data on secured, trusted devices.
- • Use a password manager approved by your company.

⚠️ If You Suspect a Threat

Don't wait. Contact your IT team or manager immediately. It's better to report a false alarm than to miss a real threat.

This guide was created by FRCS Tech to help teams stay secure and confident online.
Visit www.frcstech.com for more resources.