Phishing & Social Engineering Quick Reference

Phishing is the #1 attack vector, responsible for over 90% of data breaches. Attackers impersonate trusted entities via email, phone (vishing), text (smishing), and social media. This guide arms you with the knowledge to identify and report these attacks before they succeed.

Key Points

- ✓ Verify sender email addresses carefully — look for misspellings and domain swaps (e.g., @micros0ft.com)
- ✓ Hover over links before clicking to inspect the actual destination URL
- ✓ Be suspicious of urgency tactics: "Act now or your account will be locked"
- ✓ Never provide credentials via email, chat, or phone — legitimate services never ask this way
- ✓ Watch for poor grammar, generic greetings, and mismatched branding in messages
- ✓ Verify unexpected requests through a separate, trusted communication channel
- ✓ Report all suspicious messages immediately — do not delete them

Action Items

1. Enable email filtering and anti-phishing protection on your email client today
2. Set up multi-factor authentication on all business-critical accounts
3. Bookmark your organization's official phishing report link or email address
4. Practice the "STOP, LOOK, THINK" method before clicking any link in emails
5. Share this guide with at least one colleague this week

Quick Reference

Phishing Red Flags: Unexpected urgency, mismatched sender/domain, generic greeting, suspicious links, spelling errors, requests for credentials or payments.
When in doubt: Do NOT click. Forward the message to your security team and delete it.
Report to: security@yourcompany.com or use the "Report Phishing" button in Outlook/Gmail.