General Phishing Awareness & Prevention

Step 1: Think Like a Scammer

If the message uses fear, urgency, or pressure from authority, treat it as suspicious. Before reacting to any unexpected message, ask:

- ☐ If I were trying to trick someone, would I use a logo that looks almost correct?
- ☐ Would I copy the tone and branding of a company people trust?
- ☐ Would I create panic? (“URGENT: Account compromised”)
- ☐ Would I use deadlines or threats? (“Service shut down in 24 hours”)
- ☐ Would I claim authority? (“Final notice from the IRS”)

Step 2: Phishing Red Flag Checklist

Run through this list before clicking anything.

Sender Details

- ☐ The email address matches the real company domain exactly
- ☐ No swapped letters or numbers (e.g., amaz0n, paypal, micr0soft)

Greeting

- ☐ Uses my actual name or the correct company name
- ☐ Not generic (“Dear Customer,” “User,” “Account Holder”)

Tone & Pressure

- ☐ No extreme urgency (“Respond in 1 hour”)
- ☐ No threats of immediate loss or shutdown
- ☐ No scare tactics about legal action or account closure

Writing Quality

- ☐ No obvious spelling errors
- ☐ No strange grammar or awkward phrasing
- ☐ Formatting looks professional and consistent

Links & Attachments

- ☐ I hovered over links, and the URL matches the real site
- ☐ The domain name is spelled correctly
- ☐ No random strings of letters/numbers in the link
- ☐ I am expecting this attachment
- ☐ The file type makes sense (not .zip, .exe, or unknown files)

Sensitive Information Requests

If any box above cannot be checked, stop. Do not click.

- ☐ The email does NOT ask for passwords
- ☐ The email does NOT request banking details
- ☐ The email does NOT request Social Security numbers

Step 3: Safe Response Protocol

If something feels off:

- ☐ Do NOT click links
- ☐ Do NOT open attachments

- ☐ Do NOT reply to the email
- ☐ Verify directly with the company using their official website or phone number
- ☐ Report the email internally (manager or IT contact)

Mastectomy Business Protection Checklist

Staff Training

☐ Phishing awareness included in onboarding
☐ Ongoing refresher training scheduled
☐ Staff encouraged to question suspicious emails
☐ Incentives for reporting phishing attempts

Account Security

☐ Multi-Factor Authentication (MFA) enabled on all accounts
☐ MFA required for email, billing systems, EMR, and vendor portals

Systems & Software

☐ Automatic updates enabled
☐ Operating systems up to date
☐ Antivirus/endpoint protection active
☐ Browsers and plugins updated

Password Practices

☐ Password manager in use
☐ Unique password for every system
☐ No passwords stored on paper or sticky notes
☐ No shared logins among staff

Incident Reporting

☐ Suspicious emails reported to the FTC
☐ Phishing attempts submitted to reporting services (e.g., PhishTank)
☐ Impersonated companies notified
☐ Internal log of phishing attempts maintained