1. Introduction (5 mins)
   1. Personal Intro (Who am I?)
      * Owner of Testra
        + Started as Safety Starts Here
      * Long-time computer hobbyist
        + Self taught for over 20 years
      * Amateur Game/Website builder
        + Several published websites and an ongoing game project
   2. Why is this topic important?
      * Scam Emails/Calls
        + How to spot a scam
        + What to do about a scam
        + Future prevention
      * Phishing
        + What is Phishing
        + How to spot a phisher
        + Future prevention
      * Personal Information sellers
        + Confirm before handing information out
        + Trusted sites only
        + DO NOT accept all cookies
        + Public Vs Private info
   3. Session overview:
      * Common tricks and scams
        + Impersonators
          1. Tech Support
          2. Family
          3. Government / Police
        + Exploiting urgency
          1. Buy now save later
          2. Bait and switch
          3. Limited offers
        + Web Stores/Marketplace
          1. Money upfront
          2. Free offers w/ credit card information
          3. How to use safely
        + Examples found recently
      * Common bad habits
        + Weak passwords
          1. Reused, simple or short
          2. 2-Step Authentication 2FA
2. Most Common Tricks (15 mins)
   1. Phone scams and automated calls
      * Robot callers claiming you’ve won a prize, or pretending to be your bank/government/family.
      * Caller ID spoofing, don’t immediately trust the name because you know it
   2. Phishing emails
      * Often disguised as delivery updates, account warnings, or refund offers.
      * Spelling errors, mismatched sender addresses, links that don’t match the company website.
      * Asking you to sign-in to dispute a matter, possibly a strange sign-in area
   3. Pop-up
      * Fake virus alerts or “Your computer is infected!” messages
      * They push urgency “Click now or your files will be deleted.”
      * Legit companies don’t use pop-ups to demand immediate action.
   4. Sponsored Sites
      * Upper listed links labeled as “Sponsored”
      * Just never use them, can usually scroll down and find a real link
3. Common Bad Habits (10 mins)
   1. Passwords
      * Don’t use “1234”
      * Don’t use pet or relative’s names
      * Write them in a safe notebook or password manager
      * Explain why your email should be a **unique** and **strong** password.
   2. Two-Step Authentication (2FA)
      * Explain why you should use 2FA for important log-ins.
      * Show an example of how to create and use a 2FA for email.
   3. Think before you click
      * Don’t click suspicious and/or unsolicited emails
      * Verify if necessary, by phone/walk-in
4. Group Activity (10 mins)
   1. Show 3 examples on screen/printouts:
      * A fake email
      * A fake bank text
      * A real email vs the fake one
   2. Ask: *“Who thinks this one is real? Who thinks it’s fake?”*
   3. Walk through why it might be fake
      * Address
        + Check sender email/number
      * Spelling
        + Errors are common in scams
      * Urgency
        + Phrases like “Immediate Action Required”
        + Click here to verify or sign-in
      * Logo / signature.
        + May look slightly off (Pixelated or outdated)
5. Safe Device Use/Connections (5 mins)
   1. Keep your computer/phone updated (explain “updates are like vaccinations”).
      * Updates patch security holes
      * Internet browsers need updates too
   2. Use home Wi-Fi, not random café Wi-Fi. (Why?)
      * Password protected, private WiFi is always safer
      * Strangers can see your activity on public WiFi connections
   3. Don’t install apps or click things you don’t understand.
      * Only use official app stores
        + Apple Play Store
        + Google Play
        + Microsoft Store
      * Avoid pop-up download links
      * Analogy: *“You wouldn’t take candy from a stranger, don’t take apps or links from one”*
6. Social Media & Sharing (5 min)
   1. Don’t post vacation dates before you go (Atleast not publicly)
      * Criminals will target your home
      * Post photos after returning or viewable by friends only
      * Share photos privately or after returning
   2. Be wary of friend requests from strangers, or from friends you are already have added previously
      * Be cautious of duplicates
        + Scammers copy friend’s profiles to trick you
        + Confirm with the friend directly if it’s suspicious
   3. Don’t sign-in to suspicious sites using Facebook or Google
      * Scammers often sell data collected from such sites
7. Wrap-up / Q&A (10 mins)
   1. Summarize key points
      * Strong passwords
        + Unique and not re-used
      * Be suspicious of calls/emails asking for money
        + Verify through safe means
      * Updates & safe browsing
        + Keep devices and browsers current
        + Don’t overshare online
   2. Provide a short checklist to take home
      * Password tips
      * Safe clicking tips
      * Social media tips
      * 2FA setup instructions
      * Apps to keep updated
   3. Open Q&A
      * Invite audience to share experiences
        + Go over what they could/should have done or did
      * Encourage asking yourself “Is this safe” when unsure browsing online