PHISHING AWARENESS TRAINING

WELCOME TO THE PHISHING AWARENESS TRAINING

BY: DIVYA DESHMUKH

WHAT IS PHISHING?

- **WHAT IS PHISHING?**

  PHISHING IS WHEN SOMEONE TRIES TO TRICK YOU INTO GIVING THEM PERSONAL INFORMATION, LIKE PASSWORDS OR CREDIT CARD NUMBERS, BY PRETENDING TO BE SOMEONE YOU TRUST, SUCH AS A BANK OR A POPULAR WEBSITE.

DIFFERENT TYPES OF PHISHING:

- **EMAIL PHISHING** – FAKE EMAILS PRETENDING TO BE FROM A TRUSTED SOURCE.
- **WHALING** – PHISHING AIMED AT HIGH-LEVEL INDIVIDUALS, LIKE CEOS OR EXECUTIVES.
- **SMISHING** – PHISHING VIA TEXT MESSAGE.
- **VISHING** – PHISHING OVER THE PHONE.
- **SPEAR PHISHING** – A MORE TARGETED ATTACK, OFTEN AIMED AT SPECIFIC INDIVIDUALS.

WHY SHOULD YOU CARE?

•**Why It’s Important:**
Phishing attacks can lead to:
•Losing personal data like bank information.
•Getting your computer infected with malware (harmful software).
•Stealing money or causing harm to your company.

•**Did You Know?**
Most cyberattacks start with phishing emails. That's why it’s important to know how to spot them!

HOW PHISHING WORKS

- **HOW IT HAPPENS:** SOMEONE SENDS YOU AN EMAIL OR MESSAGE PRETENDING TO BE FROM A COMPANY OR PERSON YOU TRUST.
- THEY ASK YOU TO CLICK ON A LINK OR DOWNLOAD AN ATTACHMENT.
- WHEN YOU DO, THEY STEAL YOUR PERSONAL INFORMATION OR INSTALL HARMFUL SOFTWARE ON YOUR DEVICE.

HOW TO SPOT PHISHING EMAILS

- **THINGS TO LOOK OUT FOR: STRANGE SENDER EMAIL:** CHECK THE EMAIL ADDRESS. IT MIGHT LOOK SIMILAR TO A REAL ADDRESS BUT WITH SMALL CHANGES.
- **GENERIC GREETING:** PHISHING EMAILS OFTEN SAY THINGS LIKE “DEAR CUSTOMER” INSTEAD OF USING YOUR NAME.
- **URGENCY OR THREATS:** IF THE EMAIL SAYS SOMETHING LIKE “YOUR ACCOUNT WILL BE LOCKED UNLESS YOU ACT NOW,” IT’S PROBABLY A SCAM.
- **SUSPICIOUS LINKS:** ALWAYS HOVER YOUR MOUSE OVER LINKS TO SEE WHERE THEY GO. IF THE WEBSITE ADDRESS LOOKS WEIRD, DON’T CLICK.
- **SPELLING OR GRAMMAR ERRORS:** PHISHING EMAILS OFTEN HAVE STRANGE MISTAKES IN THE TEXT.

HOW TO SPOT PHISHING WEBSITES

- **RED FLAGS ON WEBSITES:WEIRD URL:** ALWAYS CHECK THE WEBSITE ADDRESS (URL). IT SHOULD MATCH THE OFFICIAL WEBSITE, AND THERE SHOULD BE NO TYPOS.
- **NO "HTTPS" OR PADLOCK:** SAFE WEBSITES START WITH "HTTPS://" AND HAVE A PADLOCK SYMBOL.
- **POOR DESIGN OR GRAPHICS:** PHISHING SITES OFTEN LOOK LESS PROFESSIONAL, WITH LOW-QUALITY IMAGES OR STRANGE LAYOUTS.
- **TOO MANY ADS OR POP-UPS:** FAKE SITES MIGHT HAVE ANNOYING POP-UPS ASKING YOU TO CLICK.

WHAT IS SOCIAL ENGINEERING?

- **WHAT IS IT?**
  SOCIAL ENGINEERING IS WHEN SOMEONE TRICKS YOU INTO GIVING THEM INFORMATION BY PRETENDING TO BE SOMEONE YOU KNOW OR TRUST.
- **TYPES OF SOCIAL ENGINEERING:**
  - **PRETEXTING:** THE ATTACKER PRETENDS TO BE SOMEONE ELSE (E.G., A BANK ASKING FOR YOUR DETAILS).
  - **BAITING:** OFFERING SOMETHING FREE OR TOO GOOD TO BE TRUE (LIKE FREE SOFTWARE) TO LURE YOU IN.
  - **IMPERSONATION:** THE ATTACKER PRETENDS TO BE A COLLEAGUE OR BOSS ASKING YOU TO TAKE ACTION, LIKE TRANSFERRING MONEY.

HOW TO PROTECT YOURSELF

- **BEST TIPS TO STAY SAFE:**
  - **BE CAREFUL WITH EMAILS:** DON'T CLICK ON LINKS OR ATTACHMENTS IN EMAILS YOU WEREN'T EXPECTING.
  - **CHECK THE SENDER'S EMAIL:** MAKE SURE THE EMAIL IS FROM SOMEONE YOU TRUST. WHEN IN DOUBT, DON'T CLICK!
  - **LOOK FOR RED FLAGS ON WEBSITES:** ALWAYS MAKE SURE A WEBSITE IS SECURE BEFORE ENTERING ANY PERSONAL INFORMATION.
  - **DON'T SHARE PERSONAL INFO OVER THE PHONE OR EMAIL:** BE SUSPICIOUS OF UNSOLICITED REQUESTS FOR YOUR DETAILS.
  - **USE STRONG PASSWORDS AND TWO-FACTOR AUTHENTICATION:** THIS ADDS AN EXTRA LAYER OF SECURITY TO YOUR ACCOUNTS.

WHAT TO DO IF YOU GET A PHISHING EMAIL

- **IF YOU THINK IT'S A PHISHING EMAIL: DON'T RESPOND:** DON'T REPLY TO THE EMAIL OR CLICK ON ANY LINKS.
- **DON'T OPEN ATTACHMENTS:** DON'T OPEN ANY ATTACHMENTS THAT LOOK SUSPICIOUS.
- **REPORT IT:** LET YOUR IT DEPARTMENT OR SUPERVISOR KNOW ABOUT THE SUSPICIOUS EMAIL.
- **DELETE IT:** AFTER REPORTING, DELETE THE EMAIL FROM YOUR INBOX.

REAL-LIFE PHISHING EXAMPLES

- **Example 1:**
An email that looks like it's from your bank saying, "Your account is locked. Click here to verify your identity."
- **Example 2:**
A text message offering a "free iPhone" if you click a link and enter your personal information.
- **Example 3:**
A fake website that looks like Amazon, offering huge discounts to steal your credit card details.

KEY TAKEAWAYS

•**Remember:**

•Always double-check the sender and the links in emails.
•Don’t give out personal info unless you are sure the request is legitimate.
•Keep your devices updated with the latest security patches.

•**What You Can Do:**
•Stay aware of phishing threats and always be cautious with your personal information!

THANK YOU