Phishing Awareness Training

Phishing is a form of cybercrime where attackers use deceptive emails, websites, and social engineering tactics to steal sensitive information like login credentials, financial data, and personal details. This training will help you recognize and avoid these sophisticated scams.

BY: Gaurav Pal

TO: code_Alpha

Understanding Phishing Attacks

1 **Lure**

The attacker crafts a tempting message or website to lure the victim.

2 **Exploit**

The victim is tricked into revealing sensitive information or downloading malware.

3 **Monetize**

The attacker uses the stolen data for financial gain or further attacks.

Recognizing Phishing Emails

1. **Suspicious Sender**

   Check the email address - does it look legitimate?

2. **Urgent Tone**

   Phishing emails often create a false sense of urgency.

3. **Generic Greetings**

   Phishing emails often use generic salutations like "Dear Customer".

4. **Attachments/Links**

   Be wary of unsolicited attachments or links that could contain malware.

Identifying Malicious Websites

URL Inspection

Look for misspellings, unusual domains, or suspicious-looking URLs.

SSL Certificate

Verify the website has a valid SSL certificate and "https://" prefix.

Visual Cues

Check for poor design, stock images, or other signs of a fake website.

Social Engineering Tactics

Pretexting

Attackers create a plausible scenario to manipulate victims into sharing information.

Baiting

Leaving behind infected physical media like USB drives to lure victims.

Tailgating

Physically following someone into a restricted area by blending in.

Phishing

Using deceptive emails, messages, or websites to steal sensitive data.

Best Practices for Avoiding Phishing

Verify

Confirm the source of any suspicious emails or messages.

Inspect

Carefully examine URLs, attachments, and websites for signs of fraud.

Report

Notify the appropriate authorities about any suspected phishing attempts.

Educate

Stay informed about the latest phishing tactics and share knowledge.

OMMON TYPES OF PHIS

NG
te
onate
nies
teal
on.

SPEAR PHISHING
Similar to email phishing, but the messages are more personalized. For example, they may appear to come from your boss.

CLO
Sca
an
rece
att

WHALING
ers target high-ranking
tives to gain access to
itive data or money.

POP-UP PHISHI
Fraudulent pop-u
trick users into
installing malwar

Reporting Suspected Phishing Attempts

1

Identify

Recognize the signs of a phishing attempt.

2

Document

Collect evidence like screenshots and email headers.

3

Report

Notify your organization's IT team or the appropriate authorities.

TO CATCH THE ONLINE SHA
HO ARE PHISHING FOR YOU

Fraudster "sharks" are pl
for your private informatio
fake emails and webs

These criminals cause 40% of healthcare privacy
breaches. They steal our personal info and patients
our identities, and abuse credit cards and ban

Watch out for these signs!

F A PHISHING EMAIL

om" address:
mail address may look official
ring your mouse over the
yperlinked address is
he message is probably fake.
asks for personal
n: Reputable firms don't ask
sswords, credit card info, SS
tc.
threats, fear & urgent
make you act instantly.
as poor spelling or grammar;
eems awkward.
unknown, greeting is vague
s are vague.
suspicious request to click a
n an attachment.
doesn't match sender details.
ces from unknown senders.
confirmed identity.
through.

SIGNS OF A PHISHING

- **Insecure websites:** Secure
in your browser's address b
start with https://and a sec
HTTP-based URLs are often
- **Fake websites:** Watch for m
irregular web addresses, e.g
paypa1.com (number 1 inst
l). Even if a site looks real
company logo, check for a
on the bottom, especially if
transaction or giving perso
- **Man-in-the-middle** phishing
link from social media sites
to a fake page that then as
information or a transaction
- **Malicious websites** with att
offers found via search eng
Offer seems too good to be
probably was created to ste

ere

www.medsphere.com

Conclusion and Resources

1 **Stay Vigilant**

Phishing attacks are constantly evolving, so remain cautious.

2 **Ongoing Education**

Regularly review phishing prevention best practices and resources.

3 **Report and Respond**

Notify the proper authorities if you suspect a phishing attempt.