LAB Manual

PART A

(PART A: TO BE REFFERED BY STUDENTS)

**Experiment No: 7**

**A.1 Aim:**

To study the anatomy of Email Phishing

**A.2 Prerequisite:**

Fundamentals of Email Phishing

**A.3 Outcome:**

**After successful completion of this experiment students will be able to** 1. Understand types of Phishing attacks.

2. Protect our data / resources from different email phishing.

3. Identify phishing email

**A.4 Theory:**

Phishing is the fraudulent attempt to obtain [sensitive information](https://en.wikipedia.org/wiki/Sensitive_information) or data, such as usernames, passwords and [credit card](https://en.wikipedia.org/wiki/Credit_card) details, by disguising oneself as a trustworthy entity in an [electronic communication](https://en.wikipedia.org/wiki/Electronic_communication). Typically carried out by [email spoofing](https://en.wikipedia.org/wiki/Email_spoofing), [instant messaging](https://en.wikipedia.org/wiki/Instant_messaging), and text messaging, phishing often directs users to enter [personal information](https://en.wikipedia.org/wiki/Personal_information) at a fake website which matches the [look and feel](https://en.wikipedia.org/wiki/Look_and_feel) of the legitimate site.

Phishing is an example of [social engineering](https://en.wikipedia.org/wiki/Social_engineering_(computer_security)) techniques used to deceive users. Users are lured by communications purporting to be from trusted parties such as [social web sites](https://en.wikipedia.org/wiki/Social_networking_service), [auction sites](https://en.wikipedia.org/wiki/Online_auction), banks, colleagues/executives, [online payment processors](https://en.wikipedia.org/wiki/E-commerce_payment_system) or IT administrators.

Attempts to deal with phishing incidents include [legislation](https://en.wikipedia.org/wiki/Legislation), user training, public awareness, and technical security measures (the latter being due to phishing attacks frequently exploiting weaknesses in current web security).

**Email Phishing:**

* Phishing is a type of online scam where criminals send an email that appears to be from a legitimate company and ask you to provide sensitive information. This is usually done by including a link that will appear to take you to the company’s website to fill in your information – but the website is a clever fake and the information you provide goes straight to the crooks behind the scam.
* The term ’phishing’ is a spin on the word fishing, because criminals are dangling a fake ’lure’ (the email that looks legitimate, as well as the website that looks legitimate) hoping users will ’bite’ by providing the information the criminals have requested – such as credit card numbers, account numbers, passwords, usernames, and more.

**Task 1:**

List the methods to identify phishing email. (Minimum One-page document)

Visit following links.

<https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams>

<https://www.securitymetrics.com/blog/7-ways-recognize-phishing-email>

<https://magma.co.in/phishing-attack/>

<https://us.norton.com/internetsecurity-online-scams-phishing-email-examples.html>

<https://www.technology.pitt.edu/security/phishing-awareness-don%E2%80%99t-take-bait>

<https://security.berkeley.edu/education-awareness/phishing/phishing-examples-archive#:~:text=Phishing%20Example%3A%20%22Dear%20Email%20User%22%20Expired%20Password%20Ploy&text=An%20example%20of%20a%20common,leads%20to%20a%20malicious%20website.>

**Task 2:**

Share the phishing email that you have received earlier (if any). (Screenshot of at least one email)

Mention the reasons: how you identify the phishing email? (One paragraph for each email)

(You can blur the content to maintain the privacy).

**Task 3:**

***Disclaimer:*** *Use these websites to understand the concept of how hackers can send spoof/fake/phishing email, do not use such website or send spoof/fake/email to anyone else. This may be considered as violation of govt. rules and regulation.*

Use this website to send sample fake email to your email address or your second email address.

(at least one email with screenshot)

<https://emkei.cz/>

<http://www.anonymailer.net/>

**Task 4:**

Visit this website, give test to identify phishing email provide.

<https://www.phishingbox.com/phishing-iq-test> (Screenshot of test result)

PART B

(PART B : TO BE COMPLETED BY STUDENTS)

***(Students must submit the soft copy as per following segments within two hours of the practical. The soft copy must be uploaded on the Portal or emailed to the concerned lab in charge faculties at the end of the practical in case the there is no portal access available)***

|  |  |
| --- | --- |
| Roll. No.: N049 | Name: Tarun Tanmay |
| Class MBATech CE | Batch: B3 |
| Date of Experiment: 22/08/2020 | Date of Submission: 27/08/20 |
| Grade: | |

**B.1 Theory written by student:**

***Provide theory as per the tasks studied in lab session over here.***

**Task 1:**

Scammers use email or text messages to trick you into giving them your personal information. They may try to steal your passwords, account numbers, or Social Security numbers. If they get that information, they could gain access to your email, bank, or other accounts. Scammers launch thousands of phishing attacks like these every day — and they’re often successful. The FBI’s Internet Crime Complaint Center reported that people lost $57 million to phishing schemes in one year.

Scammers often update their tactics, but there are some signs that will help you recognize a phishing email or text message. Phishing emails and text messages may look like they’re from a company you know or trust. They may look like they’re from a bank, a credit card company, a social networking site, an online payment website or app, or an online store.

Phishing emails and text messages often tell a story to trick you into clicking on a link or opening an attachment. They may:

* say they’ve noticed some suspicious activity or log-in attempts
* claim there’s a problem with your account or your payment information
* say you must confirm some personal information
* include a fake invoice
* want you to click on a link to make a payment
* say you’re eligible to register for a government refund
* offer a coupon for free stuff

Your email spam filters may keep many phishing emails out of your inbox. But scammers are always trying to outsmart spam filters, so it’s a good idea to add extra layers of protection. Here are four steps you can take today to protect yourself from phishing attacks.

**1. Protect your computer by using security software:** Set the software to update automatically so it can deal with any new security threats.

**2. Protect your mobile phone by setting software to update automatically:** These updates could give you critical protection against security threats.

**3. Protect your accounts by using multi-factor authentication:** Some accounts offer extra security by requiring two or more credentials to log in to your account. This is called multi-factor authentication. The additional credentials you need to log in to your account fall into two categories:

* Something you have — like a passcode you get via text message or an authentication app.
* Something you are — like a scan of your fingerprint, your retina, or your face.

Multi-factor authentication makes it harder for scammers to log in to your accounts if they do get your username and password.

**4. Protect your data by backing it up:** Back up your data and make sure those backups aren’t connected to your home network. You can copy your computer files to an external hard drive or cloud storage. Back up the data on your phone, too.

Phishing emails today rarely begin with, "Salutations from the son of the deposed Prince of Nigeria..." and it's becoming increasingly difficult to distinguish a fake email from a verified one. But, most have subtle hints of their scammy nature. Here are seven email phishing examples to help you recognize a malicious email and maintain email security.

1. **Legit companies don’t request your sensitive information via email:** Chances are if you receive an unsolicited email from an institution that provides a link or attachment and asks you to provide sensitive information, it’s a scam. Most companies will not send you an email asking for passwords, credit card information, credit scores, or tax numbers, nor will they send you a link from which you need to login.
2. **Legit companies usually call you by your name:** Phishing emails typically use generic salutations such as “Dear valued member,” “Dear account holder,” or “Dear customer.” If a company you deal with required information about your account, the email would call you by name and probably direct you to contact them via phone. BUT, some hackers simply avoid the salutation altogether. This is especially common with advertisements.
3. **Legit companies have domain emails:** Don’t just check the name of the person sending you the email. Check their email address by hovering your mouse over the ‘from’ address. Make sure no alterations (like additional numbers or letters) have been made. Check out the difference between these two email addresses as an example of altered emails: michelle@paypal.com michelle@paypal23.com Just remember, this isn’t a foolproof method. Sometimes companies make use of unique or varied domains to send emails, and some smaller companies use third party email providers.
4. **Legit companies know how to spell:** Possibly the easiest way to recognize a scammy email is bad grammar. An email from a legitimate organization should be well written. Little known fact – there’s actually a purpose behind bad syntax. Hackers generally aren’t stupid. They prey on the uneducated believing them to be less observant and thus, easier targets.
5. **Legit companies don’t force you to their website:** Sometimes phishing emails are coded entirely as a hyperlink. Therefore, clicking accidentally or deliberately anywhere in the email will open a fake web page, or download spam onto your computer.
6. **Legit companies don’t send unsolicited attachments:** Unsolicited emails that contain attachments reek of hackers. Typically, authentic institutions don’t randomly send you emails with attachments, but instead direct you to download documents or files on their own website. Like the tips above, this method isn’t foolproof. Sometimes companies that already have your email will send you information, such as a white paper, that may require a download. In that case, be on the lookout for high-risk attachment file types include .exe, .scr, and .zip. (When in doubt, contact the company directly using contact information obtained from their actual website.)
7. **Legit company links match legitimate URLs:** Just because a link says it’s going to send you to one place, doesn’t mean it’s going to. Double check URLs. If the link in the text isn't identical to the URL displayed as the cursor hovers over the link, that's a sure sign you will be taken to a site you don’t want to visit. If a hyperlink’s URL doesn’t seem correct, or doesn’t match the context of the email, don’t trust it. Ensure additional security by hovering your mouse over embedded links (without clicking!) and ensure the link begins with https://.

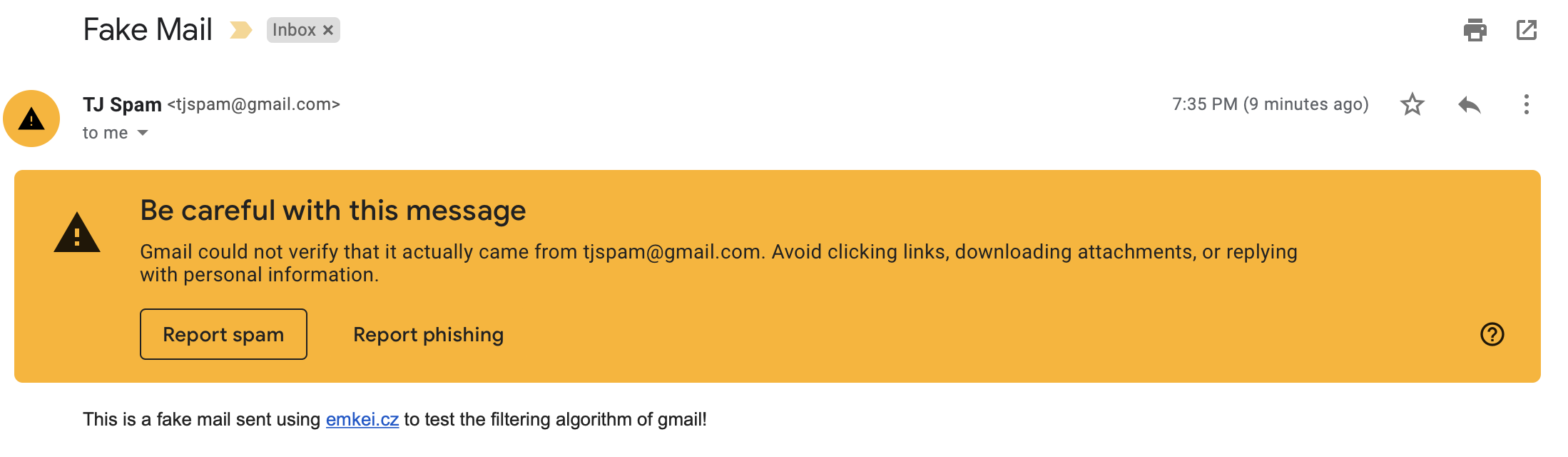
It doesn’t matter if you have the most secure security system in the world. It takes only one untrained employee to be fooled by a phishing attack and give away the data you’ve worked so hard to protect. Make sure both you and your employees understand these specific email phishing examples and all of the telltale signs of a phishing attempt.

Phishing is the attempt to obtain sensitive information such as usernames, passwords / Login Credentials, and credit / debit card details (and, indirectly, money), often for malicious reasons (usually to carry out various types of financial fraud), by disguising as a trustworthy entity in an electronic communication. The word is a neologism created as a homophone of fishing due to the similarity of using bait in an attempt to catch a victim. Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter personal information at a fake website, the look and feel of which are almost identical to the legitimate one. Communications purporting to be from social web sites , auction sites, banks, online payment processors or IT administrators are often used to lure victims. Phishing emails may contain links to websites that are infected with malware.

An attacker masquerades a trusted entity, such as a bank, government, ISP (Internet Service Provider), web site, and tries to trick people into giving up their private information. These attacks often take the form of “urgent” emails asking people to take immediate action in order to prevent some impending disaster.

* **Be careful about responding to emails that ask you for sensitive information:** You should be wary of clicking on links in emails or responding to emails/text messages that are asking for things like account numbers, usernames and passwords, or other personal/confidential information. We at Magma do not ask for this information via email.
* **Go to the site yourself, rather than clicking on links in suspicious emails:** If you receive a communication asking for sensitive information but think it could be legitimate, open a new browser window and go to the organization’s website as you normally would (for instance, by using a bookmark or by typing out the address of the organization’s website). This will improve the chances that you’re dealing with the organization’s website rather than with a phisher’s website, and if there’s actually something you need to do, there will usually be a notification on the site. Also, if you’re not sure about a request you’ve received, please contact us at customercare@magma.co.in or call us at toll free : 1800 266 3202
* **Be wary of the “fabulous offers” and “fantastic prizes” that you’ll sometimes come across on the web:** If something seems too good to be true, it probably is, and it could be a phisher trying to steal your information. Whenever you come across an offer online that requires you to share personal or other sensitive information to take advantage of it, be sure to ask lots of questions and check the site asking for your information for signs of anything suspicious.
* **Use a browser that has a phishing filter:** The latest versions of most browsers include phishing filters that can help you spot potential phishing attacks.
* Do not reply (without confirming the legitimacy of the source) to e-mails requesting for financial information, Customer information, Account information, Personal or any other confidential information etc., such mails seems to come from legitimate source but usually are meant to persuade user to send confidential data which is later used for malicious intents.
* Do not use a link in an e-mail to get to a web page, instead, type in the URL directly into your browser’s address bar.
* Be vigilant when downloading e-mail attachment on your computer. If in doubt, do not download.

**Task 2:**

****

Since the message wasn’t encrypted, it was easily identifiable

This one was flagged as well, since most messages of such formats are phishing/spam emails.

**Task 3:**

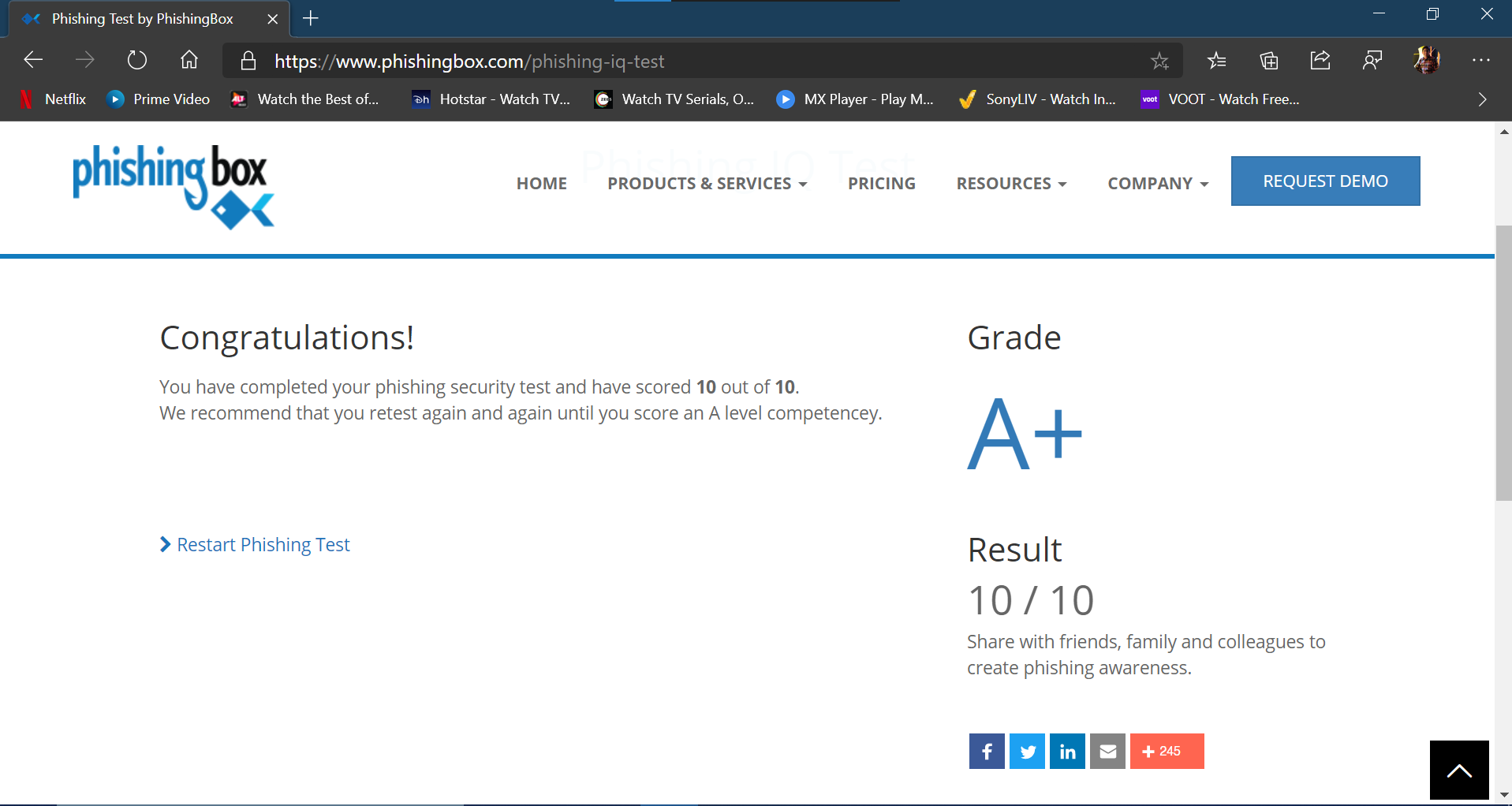
**A screenshot of a cell phone

Description automatically generated**

**A picture containing drawing

Description automatically generated**

**Task 4:**



**B.2 Input and Output:**

***(Paste your screenshot of steps all tasks assigned over here.***

<https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html>

​ <https://www.webroot.com/in/en/resources/tips-articles/what-is-phishing>

​<https://www.vadesecure.com/en/phishing-awareness-training-8-things-employees-understand/>

<https://terranovasecurity.com/top-examples-of-phishing-emails/>

**B.3 Observations and learning:**

***(Students are expected to comment on the output obtained with clear observations and learning)***

In this Experiment, we studied the fundamentals and anatomy of Email Phishing.

Phishing is the fraudulent attempt to obtain sensitive information or data, such as usernames, passwords and credit card details, by disguising oneself as a trustworthy entity in an electronic communication. Typically carried out by email spoofing, Instant Messaging and Text Messaging, phishing often directs users to enter personal information at a fake website which matches the look and feel of the legitimate site.

Phishing is an example of social engineering techniques used to deceive users. Users are lured by communications purporting to be from trusted parties such as social web sites, auction sites, banks, colleagues/executives, online payment processors or IT administrators.

Attempts to deal with phishing incidents include legislation, user training, public awareness, and technical security measures (the latter being due to phishing attacks frequently exploiting weaknesses in current web security).

The word phishing is a neologism created as a homophone of fishing.

**B.4 Conclusion:**

*(****Students must write the conclusion as per the attainment of individual outcome listed above and learning/observation noted in section B.3)***

After successful completion of this experiment I am able to understand various types of Phishing attacks. I can now protect my data/resources from different email phishing. I can also identify and distinguish phishing emails from normal emails.