**ASANSOL ENGINEERING**

**COLLEGE**

****

****

**NAME – AISHWARYA GHOSH**

**ROLL – 10800219074**

**DEPT – IT (4TH YEAR)**

**SUBJECT – CYBER SECURITY**

**SUB CODE – PEC IT 702F**

**DEPARTMENT OF INFORMATION TECHNOLOGY**

**Report Writing:**

**Topic- Phishing**

**TOPIC:**

**PHISHING**

**SUMMARY**

**Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords. The information is then used to access important accounts and can result in identity theft and financial loss.** **As widespread and well-known as phishing is now, it hasn’t been around forever. Although the practice originated sometime around the year 1995, these types of scams were not commonly known by everyday people until nearly ten years later.**

**That doesn’t mean that phishing was not a force to be reckoned with right from the start. In order to avoid falling prey to such scams yourself, it is helpful to have a basic understanding of the history behind them.**

**INTRODUCTION**

**Phishing is a type of social engineering where an attacker sends a fraudulent (e.g., spoofed, fake, or otherwise deceptive) message designed to trick a person into revealing sensitive information to the attacker or to deploy malicious software on the victim's infrastructure like ransom ware. Phishing attacks have become increasingly sophisticated and often transparently mirror the site being targeted, allowing the attacker to observe everything while the victim is navigating the site, and transverse any additional security boundaries with the victim**

**DEFINITION:**

**If you have an email account, you've probably received an email from someone you didn't know. At best, it was simply misdirected. At worst, you may have been the victim of phishing, which is the attempt to deceptively obtain personal and secured information over the internet, for the purpose of exploitation and financial gain.**

**Information typically targeted by phishing schemes includes passwords, user-names, bank account information, and social security numbers. The term 'phishing' is a play on 'fishing'-- hackers use various forms of 'bait' in order to catch a victim.**

**CONTENTS:**

* **Types of Phishing:**

1. **Email Phishing:**

**Most phishing messages are delivered by email spam, and are not personalized or targeted to a specific individual or company–this is termed "bulk" phishing.**

**Common Features of Phishing Emails :**

1. **Too Good To Be True - Lucrative offers and eye-catching or attention-grabbing statements are designed to attract people’s attention immediately. For instance, many claim that you have won an iPhone, a lottery, or some other lavish prize. Just don't click on any suspicious emails. Remember that if it seems to good to be true, it probably is!**
2. **Sense of Urgency - A favourite tactic amongst cybercriminals is to ask you to act fast because the super deals are only for a limited time. Some of them will even tell you that you have only a few minutes to respond. When you come across these kinds of emails, it's best to just ignore them.**
3. **Hyperlinks - A link may not be all it appears to be. Hovering over a link shows you the actual URL where you will be directed upon clicking on it. It could be completely different or it could be a popular website with a misspelling, for instance www.bankofarnerica.com - the 'm' is actually an 'r' and an 'n', so look carefully.**
4. **Attachments - If you see an attachment in an email you weren't expecting or that doesn't make sense, don't open it! They often contain payloads like ransom ware or other viruses. The only file type that is always safe to click on is a .txt file.**
5. **Unusual Sender - Whether it looks like it's from someone you don't know or someone you do know, if anything seems out of the ordinary, unexpected, out of character or just suspicious in general don't click on it!**

**2. Voice Phishing:**

**Voice phishing, or vising is the use of telephony (often Voice over IP telephony) to conduct phishing attacks. Attackers will dial a large quantity of telephone numbers and play automated recordings - often made using text-to-speech synthesizers - that make false claims of fraudulent activity on the victim's bank accounts or credit cards. The calling phone number will be spoofed to show the real number of the bank or institution impersonated.**

3. **SMS phishing:**

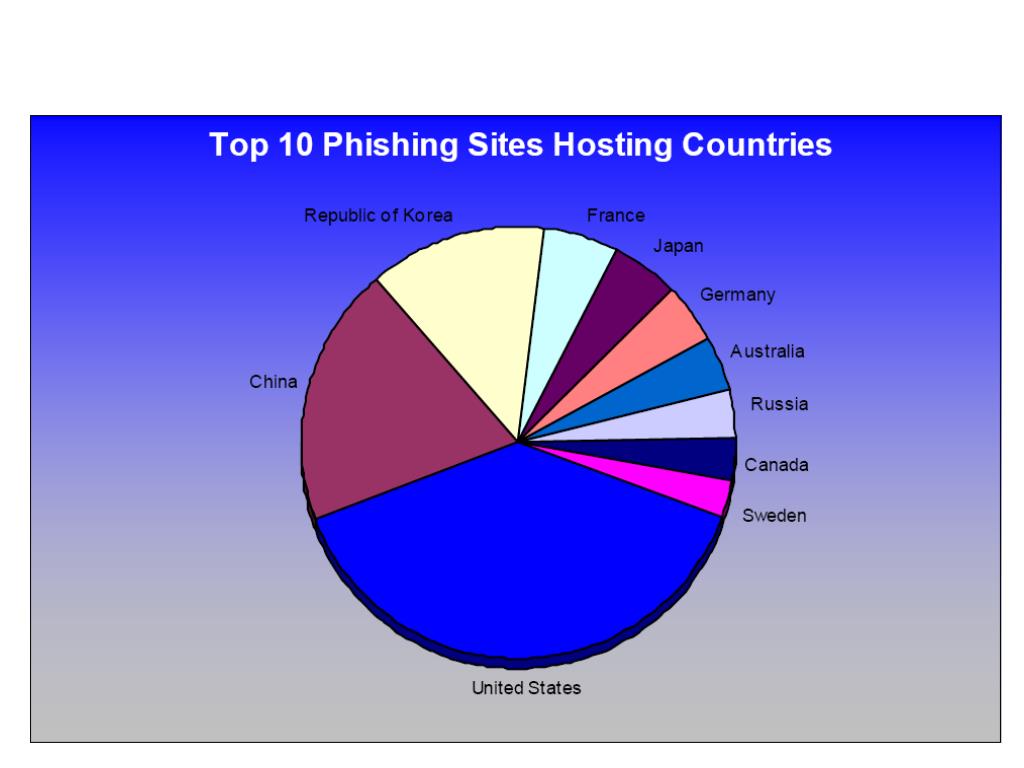
**SMS phishing or smashing is conceptually similar to email phishing, except attackers use cell phone text messages to deliver the "bait". Smashing attacks typically invite the user to click a link, call a phone number, or contact an email address provided by the attacker via SMS message. The victim is then invited to provide their private data; often, credentials to other websites or services. Furthermore, due to the nature of mobile browsers, URLs may not be fully displayed; this may make it more difficult to identify an illegitimate logon page.**

4**. Page hijacking :**

**Page hijacking involves compromising legitimate web pages in order to redirect users to a malicious website or an exploit kit via cross site scripting. A hacker may compromise a website and insert an exploit kit such as Mack in order to compromise legitimate users who visit the now compromised web server. One of the simplest forms of page hijacking involves altering a webpage to contain a malicious inline frame which can allow an exploit kit to load. Page hijacking is frequently used in tandem with a watering hole attack on corporate entities in order to compromise targets.[citation needed]**

**5.Calendar phishing :**

**Calendar phishing is when phishing links are delivered via calendar invitations. Calendar invitations are sent, which by default, are automatically added to many calendars. These invitations often take the form of RSVP and other common event requests.[36] Former Google click fraud czar Shuman Ghosemajumder believes this form of fraud is increasing, and recommends changing calendar settings to not automatically add new invitations.**



Top 10 Phishing sites Hosting Countries

**CONCLUSION:**

**What to do if you get scammed. If after all of this you still get hooked by a scammer employing a phishing tactic, there are several things you can do in order to minimize the damage that the scammer can do.**

**The very first thing you should do is contact your credit card company, as well as your bank, by phone or in person so that they can help you through the process of shutting down your cards and perhaps even moving your bank account. These companies will typically be able to track activity that is unusual and block any robbery that the scammer might try, even while it is in progress.**

**Overall, phishing is real and dangerous. Everyone needs to watch out for it because it happens to everybody; and getting scammed can be costly. Thus, be careful, follow this advice; and always keep your eyes and ears open to anything that even remotely sounds off because it may very well be scammers looking for their next victim.**

**REFERENCES:**

**There are some important sites:**

* [**www.phishing.org**](http://www.phishing.org)
* [**www.cybersecurityguide.org**](http://www.cybersecurityguide.org)
* [**www.fortinet.org**](http://www.fortinet.org)