Phishing Awareness Content

Phishing is a type of attack whose goal is to steal private information, such as login credentials or credit card numbers, usually to carry out various types of financial fraud. An attacker impersonates a trusted entity, such as a bank, government, ISP. or large 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. Examples include topics such as the following:
"Our bank has a new security system. Update your information now or you won't be able to access your account."
"We couldn't verify your information; click here to update your account."
Sometimes the email claims that something awful will happen to the sender (or a third party), as in "The sum of Rs. 30.000.000 is going to go to the Government unless you help me transfer it to your bank account."
People who click on the links in these emails may be taken to a phishing site - a web page that looks like a legitimate site they've visited before, but is actually controlled by an attacker.
Because the page looks familiar, people visiting these phishing sites enter their username, password, or other private information on the site. What they've unknowingly done is given a third party all the information needed to hijack their account, steal their money, or open up new lines of credit in their name. They just fell for a phishing attack.
The concept behind such an attack is simple: Someone masquerades as someone else in an effort to deceive people into sharing personal or other sensitive information with them.
Phishers can masquerade as just about anyone, including banks, email and application providers, online merchants, online payment services, and even governments. And while some of these attacks are crude and easy to spot, many of them are sophisticated and well-constructed. That fake email from "your bank" can look very real; the bogus "login page" you're redirected to can seem completely legitimate.
If you think you may have encountered a phishing site. please report the suspicious site to us.
What you can do to avoid phishing attacks

The good news is there are things you can do to steer clear of phishing attacks and phishing sites:
• 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 that are asking for things like account numbers, user names and passwords, or other personal information. We at BACL 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 visit our website www.bajajautocredit.com Select the (Email Us) tab and follow the directions to get your query resolved.
• 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.

How to Identify the such Phishing Mails –

- Look for poor and inappropriate grammar
- Look for generic salutations
- Look for sense of urgency
- Look for Inappropriate mail body
- Look for generic and bogus subject lines
- Look for inappropriate domain names