Security Tips

As part of our continuing sharing with customers, we have some security tips for you.

What Is Phishing?
Phishing uses spam email to trick users into divulging personal information that can then be used by hackers to wreak havoc including data theft.

A phishing attacker aims to either:

- Acquire personal identifiable information (examples: User IDs, Passwords, Credit Card Numbers);
- Install malware on victim's device;
- Commit theft of trade secrets and confidential documents.

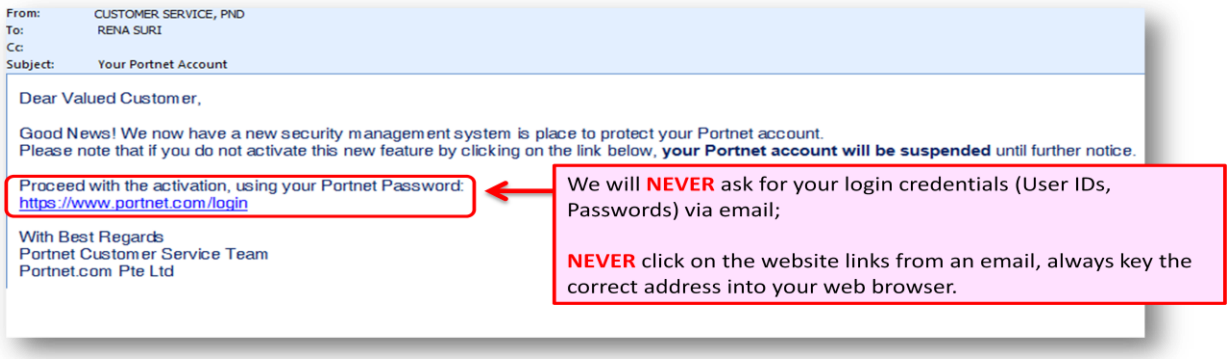
Here are 4 tips to identify a phishing email:

- **Tip 1: Don't trust the display name or header from email address**
  Appear to come from a company (e.g. PSA) you have a working relationship with & may even spoof the sender, e.g. 'Portnet Customer Service'.

- **Tip 2: Look but don't click**
  Hover your mouse over any links embedded in the body of the email. If the link address looks weird, don't click on it.

- **Tip 3: Beware of urgent or threatening language in the subject line**
  Invoking a sense of urgency or fear is a common phishing tactic. Beware of email content that claimed your "account has been suspended".

- **Tip 4: Don't believe everything you see**
  Just because an email is convincing and a seemingly valid email address, does not mean that it's legitimate. Be skeptical —if it looks even remotely suspicious, don't open it.



End