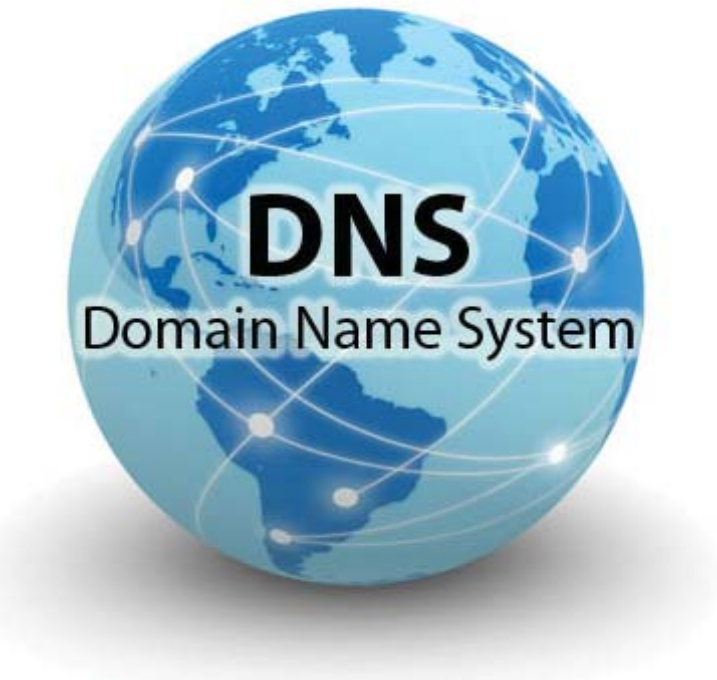
DNS AMPLIFICATION ATTACKS

THE LASTEST TREND IN CYBER MISCHIEF

DNS amplification attacks are on the rise. Are you unknowingly helping the bad guys?

An amplification attack is when a small DNS query is sent to an open, recursive DNS server. This is a devious way to return a very large answer to a small query. The purpose is to overwhelm servers and create so much traffic that it slows or blocks legitimate service use. If your DNS is open, there is a good chance that cyber criminals are stealing your resources to attack someone else.

XO has noticed a significant rise in the number of our customers with open recursive servers which forward DNS queries through the XO network, thus unknowingly participating in DNS attacks.



We are asking our customers to check if they have open servers and take the necessary steps to close them down for use only by legitimate users.

What can you do?

If you have an open recursive DNS server, evaluate your need for it.

- If you don't need it, turn it off!
- XO offers a recursive service for our customers.
- If you feel you do need it, you should – at the very least – restrict who can use it.

The United States Computer Emergency Readiness Team (US-CERT) has published a good description of DNS amplifications attacks [link] and how to protect against them. From this bulletin, you can see why an open DNS server can be an issue to any DNS server on the Internet.

XO is not actively blocking our customers from using the XO DNS service. But when XO determines the usage is impacting the XO DNS service, we reserve the right to take action. XO's Acceptable Use Policy [link] and Terms and Conditions [link] outline the acceptable use of XO services. If a customer is in violation of the AUP or TOS we always reserve the right to block access until such time as we can partner with our customers to resolve the situation.

As always, the best antidote for mischief and cyberscum is communication and partnership between the good guys.