



# OYA Technical Services



The following information is provided by OYA's Technical Services unit to help staff avoid becoming victims of cyber-crime.

Not only is it tax time, but we also have an interesting economic climate – given these factors, we are seeing more attempts to catch individuals off guard through "phishing" and malicious e-mail activity.



Phishing is a scam which attempts to persuade e-mail recipients to click on a link that takes them to a bogus website. The website may prompt the recipient to provide personal information such as social security number, bank account number or credit card number, and/or it may download malicious software onto the recipient's computer. Both the link and website may *appear* authentic, however, they are not legitimate.

OYA's Technical Services Unit is continually monitoring the agency's email system and implementing best practice security controls for workstations, including antivirus software and firewalls, and keeping them up to date.

As an individual, following are some things you can do both at work and at home to protect yourself against cyber threats:

- Do not open e-mail messages from domains like "fedreservebank.us" or "banknetwork.us". (Note: there are many others – the list is extensive and can change every day.)
- Be suspicious of email with "System Administration" in the From: field.
- Delete these e-mails from both your Inbox and Trash.
- Do not visit unknown, unsolicited, or un-trusted websites or follow links provided by unknown or un-trusted sources.
- Do not share any personal information via e-mail – confirm the contents of such e-mail messages with your contact at the appropriate organization and do not rely on an e-mail message saying you should contact a listed individual as your contact.
- Do not download or run software from unauthorized sources.



There are always going to be individuals who take advantage of others, and there will always be unsuspecting individuals who fall "hook, line, and sinker" for phishing and other scams.

Beware -- don't swim with the phishes!