

## General Computer & Email Security Tips

### Computer Security Tips

- Keep your computer operating system up to date to ensure the highest level of protection.
- Install a personal firewall on your computer.
- Install, run, and keep anti-virus and anti-malware software updated.
- Turn your computer off completely when you are finished using it – don't leave it in sleep mode.
- Conduct online banking activities on secure computers only. Public computers (computers at internet cafes, copy centers, etc.) should be used with caution, due to shared use and possible tampering. Online banking activities and viewing or downloading documents (statements, etc.) should only be conducted on a computer you know to be safe and secure.

### Email Security Tips

- Be wary of suspicious emails. Never open attachments, click on links, or respond to emails from suspicious or unknown senders.
- Consult your financial institution for any fraud activity alerts and guidance.
- If you receive a suspicious email that you think is a phishing email, do not respond or provide any information. Send the email to a reporting email address, if available, that is provided by the legitimate source. Phishing emails that fraudulently appear to come from NACHA should be forwarded (without clicking links or attachments) to [abuse@nacha.org](mailto:abuse@nacha.org) and deleted from your email account.
- If you respond to a phishing email with personal banking information, contact your financial institution immediately.