Tips to Avoid Phishing, Spyware & Malware

- Never open e-mail from unknown sources.
- Never respond to a suspicious e-mail or click on any hyperlink enclosed in a e-mail:
  -call the person who sent the e-mail
  -if the email from the credit union call us to verify
- Educate yourself about current scams and loss prevention steps.
- Make sure you have the latest versions and patches of both anti-virus and anti-spyware software. Check this at least monthly.
- Make sure system updates are being completed. Check this at least monthly.
- Install a firewall between your computer and the internet. Your internet provider can assist your with this.
- Check your security settings & select at least medium level of security for your browsers.
- Make sure your pop-ups are turned off.
- Clean out your browsing history and cache before logging into Internet Teller.

Best Practices for Online Banking Security

- Don't store/save passwords on the computer.
- Use a strong password that contains:
  -alpha/numeric characters and symbols
  -upper & lower case characters
  -minimum of 8 characters but longer is recommended
  -no real words or names of family/friends/pets
  -use entire keyboard; avoid strings of identical characters
- Change passwords regularly & use different password for each website you access.
- Never reveal your confidential login ID, password, PIN or answers to security questions to anyone.
- Never reveal your confidential login ID, password, PIN or security questions by e-mail.
- Never share your security token.
- Report lost or stolen tokens immediately.
- Never bank online using computers at kiosks, cafes unsecured computers or unsecured wireless networks.
- Prohibit the use of shared user names and passwords for your online banking accounts.