From:	Holmes, Stuart
Cc:	Elections - WEI Support
Subject:	FW: Voting System Update
Date:	Thursday, June 22, 2017 1:27:38 PM
Attachments:	image001.png

Distribution: VRDB/Data email list

Good afternoon,

I received an alert from the EAC that they received information for a voting system vendor that they have experienced system penetration attempts through what is called "phishing". I've included the full alert below and also included a link to a Department of Homeland Security (DHS) tip card on what is phishing is and tips to prevent it:
https://www.dhs.gov/sites/default/files/publications/Phishing%20508%20compliant%20508%20compliant.pdf

October is Cyber Security Awareness Month but it is never too early to get a refresher. DHS has many educational resources available on their website: https://www.dhs.gov/publication/stopthinkconnect-government-resources

Stuart Holmes| Voting Information Systems Manager
Office of the Secretary of State
(360) 725-5794 | www.vote.wa.gov

From: Ashley Williams [mailto:AWilliams@eac.gov]
Sent: Thursday, June 22, 2017 11:10 AM
Subject: Voting System Update

Standards Board Members,

The EAC has been made aware by one voting system manufacturer that they have been experiencing an increase in system penetration hacking attempts, including social engineering attack vectors through email and phone contact. Attempts have been made to obtain voting equipment, security information and in general to probe for vulnerabilities. We wanted you all to be aware of this information and to let you know we have made all of our voting system manufacturers and Voting System Test Laboratories aware.

Thank you.

Brian