



May 18, 2017

TO: Texas A&M AgriLife Unit Heads and Business Administrators
SUBJECT: Securing Agency Account Information

Texas A&M System members are increasingly being targets of fraudulent activities. Imposter fraud via financial phishing scams are on the rise. The agencies have controls in place in efforts to prevent most of these attempts. However, we need your assistance in these efforts as scams are constantly changing.

As a reminder agency funds are to be deposited in approved depository banks only. Employees are asked to notify the fiscal office of any unapproved bank accounts containing agency funds.

We recommend adopting and maintaining the following set of best practices to protect our agencies against cybercrime:

- Do not reply to any email or pop-up message that asks for agencies financial information. Legitimate companies and government agencies do not ask for this information via email.
- Neither banking information nor credit card data should be sent via email. Information needs to be sent via protected measures.
- Do not send agency banking information directly to customers.
- If a company is requesting this information to pay electronically, contact Banking and Receivables at bar@ag.tamu.edu. Include business contact information for the company. Banking will work directly with the customer to securely set up payment information.
- Units should delete any stored or saved versions of agencies bank information.
- Any vendors that contact the units directly asking for bank routing information changes, should direct the change request to Shiao-Yen Ko via phone 979-845-4778 in AgriLife Disbursements.

Questions may be directed to Gwen Tucker, Manager Banking and Receivables, via email gktucker@ag.tamu.edu or phone (979) 862-2245.

Texas A&M AgriLife Administrative Services | <http://agrilifeas.tamu.edu/>