Preventing and Detecting Email and Online Fraud.
The Internet has transformed the way we all do business, including marketing, sales, and engaging in banking services. Unfortunately, increasing online usage has been followed by increasing online criminal activity. Protecting against email and online fraud requires adherence to sound preventative measures and practices -- a number of which are included below for your consideration.

What you should know about business email fraud and online fraud.
Hackers perpetrate scams in many ways. A common way is to send fraudulent email appearing to be from a known source (an executive of your company or a client, for example) requesting bank transactions or other financial information. Hackers can also fabricate or steal an email address and use it to invite you to click on a link to a bogus website. If you follow the email instructions from a fraudster or provide confidential information, such as your user ID, password, account number, or tax ID number, then online fraud can take place, potentially putting you and your company at risk.

By proactively enhancing your company’s security, you can reduce the risk of email fraud and online fraud and minimize threats.

Safeguard your company’s online access and password.
• Create passwords that are not easily guessed. Avoid using personal information, such as your last name or birthday.
• Use different user IDs and passwords for multiple websites.
• Don’t record or save passwords, IDs, or other sensitive information on your computer.
• Don’t share your passwords or other login credentials with anyone.
• Don’t share company user IDs. Each user must have a unique user ID and password.
• Remind users to change their passwords frequently.
• Log out or lock your computer when you are away from your workstation.
• Avoid using automatic login features that save usernames and passwords for online banking.
• Never access bank, brokerage or other financial services information at Internet cafes, public libraries, etc. Unauthorized software may have been installed to trap account numbers and sign on information leaving you vulnerable to possible fraud.

Maintain internal controls and policies.
Maintain appropriate internal controls, including segregation of duties, and periodically review them. For example, require one user to set up or initiate payments and another to approve the payments. Make sure to delete user profiles that no longer need access.
• When approving transactions, carefully review all details, paying close attention to the beneficiary routing number and account number.
• Set up customized account alerts, like balance minimums, through online banking, so you know when certain account activity takes place.
• If your company processes ACH batches, approve them individually.
• If your company initiates ACH and wire transfer payments, consider using dual control (originator and authorizer).
• Verify payment or change requests with the vendor. You could receive a fraudulent email disguised to be from a known vendor. When a payment is made, the funds are sent to the fraudster instead of the intended vendor.
• Review and reconcile banking transactions daily.
• Perform periodic risk assessments of the banking products/services your company uses, including regular reviews of user access levels, dollar limits and activity.
Defend against viruses and malware.
Most companies provide security features. Work with your company’s IT professional to:
• Scan any software downloaded from the Internet for viruses before installation.
• Ensure your computer’s operating system and software are updated on a regular basis and firewalls are in place. A firewall limits the potential for unauthorized access to a network and computers.
• Verify unused ports on your computer are closed.
• Use anti-virus and anti-malware software, and keep the software patches up to date.
• Use the latest versions of Internet browsers which have “pop-up” blockers.
• Report suspicious on-screen requests asking you to enter your PIN multiple times at log on or to have someone else log on from your computer.
• Do not log on to any website with misspellings or grammatical errors or that displays unexpected behavior.
• Verify use of a secure session (“https”) in the browser for all online banking and purchasing.

Beware of suspicious emails or phone calls.
Be suspicious of emails and phone calls purporting to be from a financial institution, government department or other agency requesting account information, account verification or banking access credentials such as usernames, passwords, PIN codes and similar information. If you are not certain of the source, do not click any links or attachments, especially with file extensions ending in .exe, .pif or .vbs.

• Use caution when you receive email messages or phone calls that:
  o Threaten to close or suspend your account if you don’t provide personal information.
  o State your account has been compromised and request you provide your account information.
  o Ask you to confirm, verify or update your account, credit card or billing information.
• IBERIABANK will never request personal or account information from you through a link within an email or a pop-up window.

If you think your company’s account has been compromised, contact your IT administrator. If the email appears to be from IBERIABANK, contact your local banker immediately.

If you suspect confidential information has been stolen.
We recommend you immediately cease all activity from computer systems that may be compromised and work with your IT professional to disconnect network connections to isolate the system from remote access. Work with your banker to:

• Disable online access to accounts.
• Change online banking passwords.
• Open new account(s) and close existing account(s) as appropriate.
• Request review of all recent transactions and electronic authorizations on the account.
• Ensure that no one has requested an address change, title change, PIN change or ordered new bank cards, checks or other account documents be sent to another address.

Maintain a written chronology of what happened, what was lost, and the steps taken to report the incident to the various agencies, banks, and firms impacted.

The information contained herein is provided only for general informational purposes. It is not intended as legal advice, nor should it be relied on as such. Security threats change constantly, and there may be other measures or practices not described herein. Accordingly, IBERIABANK makes no guaranty, representation or warranty that following any of the measures or practices contained herein will result in the avoidance or detection of email or online fraud. You are encouraged to consult with an IT professional of your choosing for matters unique to your circumstances.