CYBER SECURITY

Revised Sunday, February 10, 2019

Computer use and security is an essential part of our business. We use computers as tools just like shovels, pavers and pickup trucks. And just as we cannot pave roads without asphalt, we cannot do business without computers. Being secure with a computer is the same thing as taking care of other tools. This document will offer tips, help and warnings to help you do that. If you have any question or are unsure of anything, please contact Deanna Hinson or John Jeffries at the main office.

EQUIPMENT

This is the easy one. If you are given computers, tablets or cellphones by the company, secure them. Do not leave them visible on the seat in an unlocked truck. Place them under the seat or cover them and lock your vehicle.

PASSWORDS

This protects your computer and your email. Here are the minimum requirements: At least 8 characters, At least one upper and lower case letter, At least one special character like “$”, “1” or “!”. Do not use the “/”, “\” or “@”. The special characters can also be used in place of letters. The word “arrested” can be changed to “Arr3$t3d”. The ‘e’ becomes ‘3’ and the ‘s’ becomes ‘$’. You can use several words together as a single word. Combined with the pervious requirements, this can give a very secure password. You could use “h3GotArr3$t3d” for “He got arrested”. The more complex the better, but do not make it so complex that you forget.

There are some things that are not good ideas for passwords. If a hacker is attacking you personally, they may research you prior to the attack. This means close family members and favorite sport teams are not the best choices. Going the opposite way might make it work better. If you are a Tennessee fan, using “RollTid3” would be a hard to guess password.

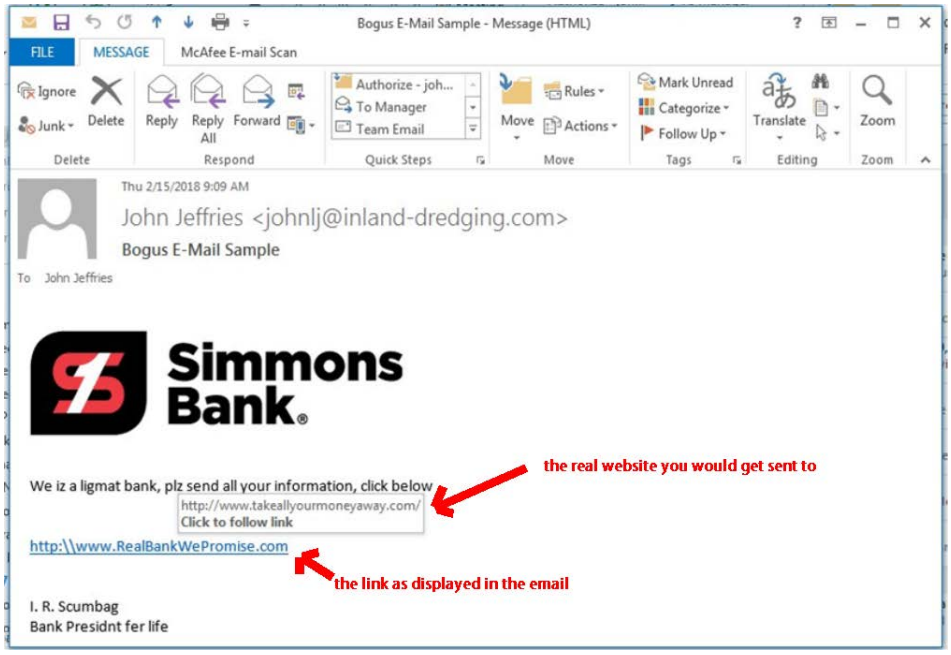
CYBER SECURITY

E-MAIL

Information flowing via email is used by management to communicate with you and with the state, banks and vendors. When that flow is stopped, it can cause problems and cost money. This is the area where the company has really been under attack. We need all employees to be aware and watchful. The bogus emails as I like to call them, can be very professional looking. Just because it has the name or log of a real company, does not make it safe. If you are unsure, forward the mail to bogus@fordcc.com and contact Deanna Hinson or John Jeffries at the main office.

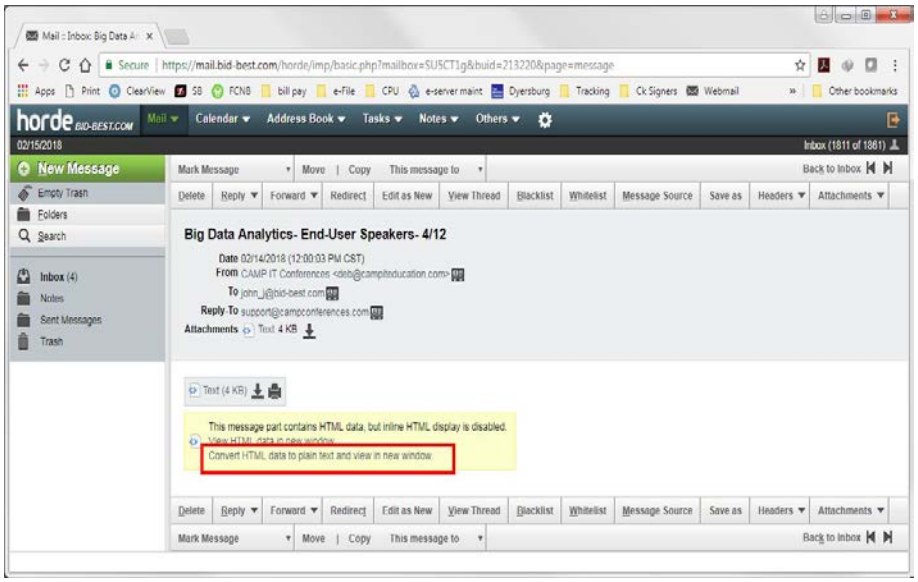
BEWARE OF UNEXPCTED EMAILS – If you were not expecting an email, verify it first. Do not verify by replying to the email. Create a new email, make a phone call or send a text to the sender asking them if they sent the email. Do not open any attachments or click on any links in an unverified emails.

CHECK OUT LINKS – Most email programs like Outlook and Thunderbird, you can pass your cursor over a link (DO NOT CLICK ON IT) and it will show you the true address in the link. In the following image, you can see that the name shown is not the actual web site it would send you to.



CYBER SECURITY

You can also use the webmail to view the email in a safe window. The webmail system has an option to convert HTML to text and display. This will allow you to read part or all of the contents, but not run any App (possible virus) inside.



DO NOT BELIEVE THREATS – Bogus email will often make a threat to deny some service or cost you money. They use phrases like "your account will be closed" or "your order has been placed" (when you did not order anything). This is designed to panic you into using their links. Do not believe it and do not do it. If you are worried, go ahead and verify, BUT NOT USING THEIR EMAIL. Contact the person, business or government agency. The company controls your computer and email accounts. You will hear verbally from us if there is an issue. And the IRS and business send certified mail via the US Post Office and do not demand payment over email.

IMPORTANT: WHAT SHOULD I DO IF AN EMAIL WAS OPENED AND/ OR A LINK CLICKED ON?

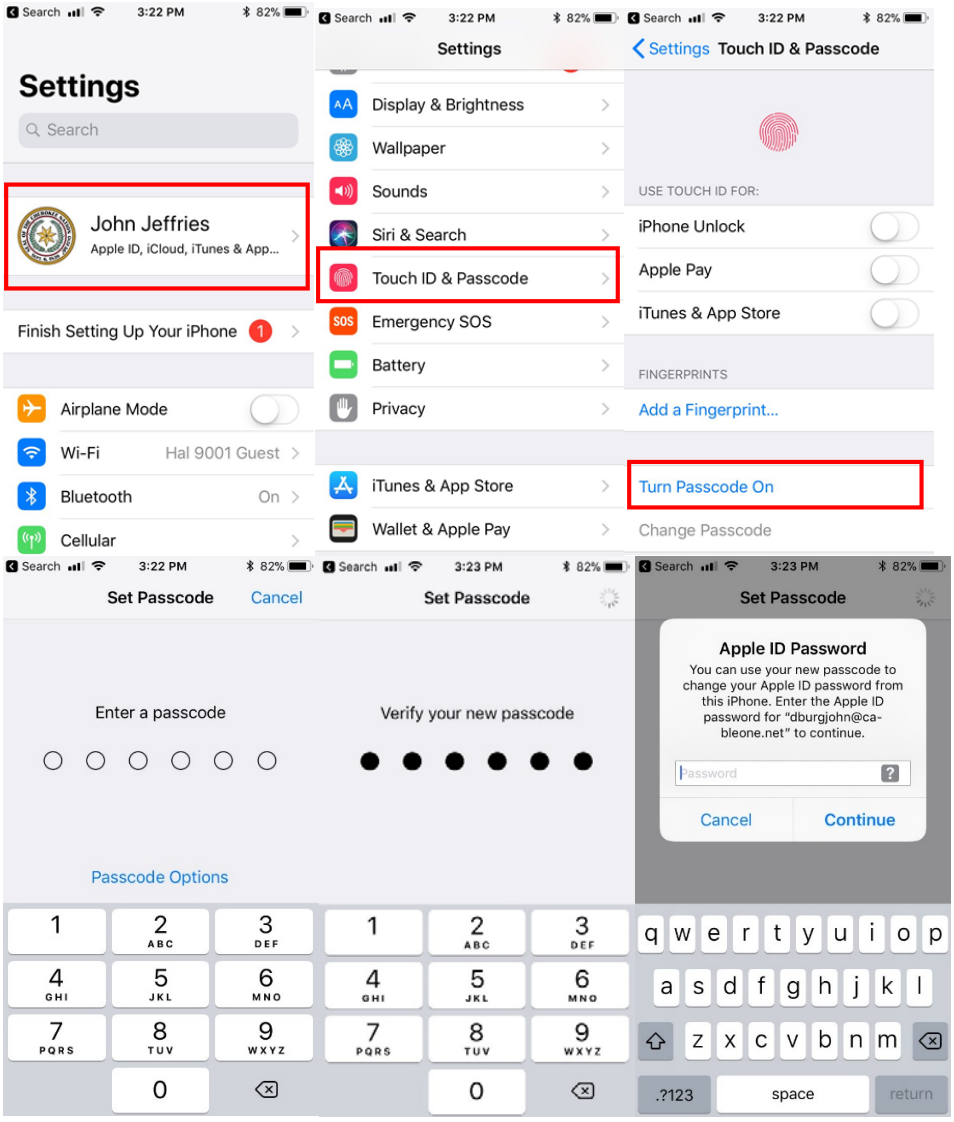
This has happened to us. The most important thing is to prevent any further damage. Cut your computer off right away. Hold the power button until it goes off. Then notify the following people: Your supervisor, Deanna Hinson, John Jeffries and for RFW staff, notify Twin Oaks.

Your computer will need to be scanned to ensure not virus code has been attached or any files compromised. We will work to return the computer to service as soon as possible. If access to a computer is time sensitive to you, a temporary replacement will be provided.

CYBER SECURITY

CELLPHONE SECURITY

The company cellphone security policy applies to all company issued phones and any personal phone which you use to access your company supplied email (fordcc.com, bid-best.com, choctawtrans.com, inland-dredging.com and rfwgroup.com). You need to protect the phone with a passcode and activate the "find my phone" option. Company provided phones are mostly Verizon. If you wish to turn the passcode on, follow the screens below.



Any Verizon store will also be happy to help you. Deanna Hinson and John Jeffries at the main office will also help you do this.