To: All Employees

From: Marland Taylor

Re: Home Network Security Best Practices

While everyone continues to Shelter-In-Place in response to Covid-19, many of us are relying on Virtual communication as a means to stay in touch with the “outside world” and for “working from home”. In support of this, it’s critical that you ensure your home network is as secure and private as it can be. The following best practices can be used as a guide (or reminders) to keep your home network safe and secure, I encourage you to follow these best practices as well as any information you may receive from your Internet Service Provider regarding privacy and security.

Things you can do:

* Change your network password at least once per month
* Always make sure you’re connected to your network (and not the neighbors unprotected network 😊)
* Never perform financially sensitive transactions over a public network, this should only be done from an Eden location or from your home
* Always verify sensitive transactions with a phone call to the requestor to avoid scam (bogus wire transfer requests is a very common scam targeting Accounting/Finance/Executive staff)
* Stay current with security patches and software updates for all devices that connect to your network (this includes updating your mobile phone)

Other tips and tricks:

* Never open an email and/or attachment that is not familiar to you (feel free to forward any suspect emails to the Eden BT help desk prior to opening, we will analyze them for you)
* Only visit web sites that are familiar to you
* Always use a password when hosting video/audio conferencing tools (if available)
* Frequently check to make sure no unauthorized devices are connected to your network

Here are some additional things you can do (if needed, you can contact your Internet Service Provider - Comcast, AT&T, Charter, etc., for assistance):

* Change your Network password
* Make sure your router admin credentials have been updated/changed since your account was originally established
* Rename and/or hide your network name
* Turn on “encryption”
* Turn off “plug and play”
* Turn off “remote management”

For more details on these, which you can discuss with your Internet Service Provider if appropriate, please see below.

1. Create a complex Router password and change it frequently as required. Many of us have regular visitors that ask for our password so they can leverage the wi-fi while visiting. Over time, your password is known by more and more people. Make your password a random sequence of letters, numbers and special characters, mixing uppercase and lowercase so no one could ever remember it. Fortunately, once a password is successfully entered into a device, it is not visible, so the people you give it to won’t be able to read it off to tell someone else. Ideally, the password should be at least 12 characters. When asked by visitors for your password, read it to them, **Do Not** write it down for them. You should store your password in a secure location at your home.
2. Change your Router’s Admin Credentials. Most routers are delivered from your provider with a default user name and password, usually given to you at the time of setup. It’s critical that you immediately change these default by accessing your router’s console from any device connected to it. Once connected, change the password of the admin account to a random string of letters and numbers and make it at least 12 characters long. Don’t forget to write that new password down in a safe place before you log out of the console.
3. Change your Network name and HIDE it. When your router is set up by your provider, they provide a default network name or SSID.  A hacker can use the information that appears in the SSID to look up the default username and password for the router with little effort. Change the SSID so that it doesn’t give away the router brand or model. Don’t choose an identifier that includes your name, address, or telephone number. **Don’t use any other personal information in the name**. Choose a very bland name that would not offer any information about you, your family or your home. Once you have renamed it, HIDE your network. Your router doesn’t have to broadcast its SSID. If you block your router from sending out its identifier, your home Wi-Fi becomes a hidden network. Those devices that already have connection data stored will still be able to connect, but passers-by won’t see it. In many cases, the network list that others see will include a line that says “Hidden network.” Without knowing the name of the network, it is impossible to connect to it.  If you have new devices that you want to add, you can temporarily turn on the SSID broadcast to let your new device see the network. Once you have set up a connection with the password, make the network hidden again. Hiding the network makes it easier to block visitors from getting on the network. If they can’t see your router in their list of available networks, they will be less likely to ask for the password.
4. Make sure your Router is using the highest level of encryption available. Three types of WI-FI protection systems are commonly used to secure transmissions so only the end user’s device and the WI-FI router can read the contents of a transmission. These are Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA 2). Of these three, you should be using WPA2 or WPA2 AES. You can change the WI-FI encryption in the router console. The AES encryption option often appears in a second pick-list. So after you choose WPA2 in the first field, you can select AES in the second field.
5. Turn off Plug and Play capability. With the abundance of “smart” appliances and other devices in homes today, routers are used to connect the appliance with the manufacturer. The feature that does this is called UPnP, it is used to get a device set up on the network and connected to the manufacturer. But once you have that thing working, switch off its UPnP capabilities. You should also turn off UPnP compatibility in your router.
6. Turn off remote management. The console of a router should only be accessible from devices connected to the network. However, a standard router setting enables remote access. This means that you can access the console over the internet, from another location. Unfortunately, if you can do that, so can anyone else. So, turn off remote access.

Thanks in advance for your support in keeping the Eden Housing computing environment safe and secure.