USB THREATS >>>

YOUR WORK STATIONS AND…

USB threats

How to help prevent USB data breaches:

Although most workstation USB ports are turned off:

- *Never insert an unknown device into your computer.*
- *If you find a random USB device laying around, immediately turn it into your IT or compliance department.*
- *Never accept and insert devices given to you by customers.*

FRAUDSTERS + USB DEVICES

We make it easy for them!

SCENERIO: You find a USB device somewhere in the lobby of your office labeled PAYROLL 2017, PASSWORDS or even CEO, what do you do with it?

If you answered this question the same way sixty percent of people would, you would pick it up and plug it into your computer to see what was on it and where it would need to go. Without even knowing it, you may have just given hackers access to your whole entire computer and if it's a business, their entire network.

USB's may *look* unassuming but can be deadly to your computer. Even with the USB ports turned off at a workstation, some USB's are able to register themselves as USB keyboards to the computer, therefore, allowing access.

The Rubber Ducky

- ✓ Works even when USB ports are off
- ✓ Registers itself as a USB Keyboard
- ✓ Sends all information back to a hacker

The Bash Bunny

- ✓ Works even when USB ports are off
- ✓ Registers itself as a Nework Card
- ✓ It is also considered the fastest route for information to travel through
- ✓ The computer will automatically reroute all traffic through this device. Ultimately delivering it directly to the hacker

The LAN Turtle