Tualatin Valley Water District

Mobile Electronic Device Security

Pete Boone, PE, PLS – Tualatin Valley Water District

Presentation Overview

Importance of device security

Types of devices

Types of data

Keeping devices and data secure

Importance of Security

Recent incidents in the news:

- February 2013 – Laptop stolen from OHSU surgeon. Data on 4,000 patients lost.
- February 2013 – Laptop stolen from VA Medical Center in South Carolina. Data on 7,000 patients lost.
- February 2013 – Laptop stolen from Canadian Investment Regulatory Organization employee. Data on 57,000 investors lost.
- April 2013 – Laptop stolen from Rutgers University graduate student. 5 years of research data lost just weeks before his master's degree thesis defense. Offered $1,000 reward for the return of his data.

Importance of Security

Devices are generally targeted by thieves for easy money, but they could be after the data or network access.

More of us are using a laptop as our primary computer.

As we become more dependent on our digital devices, they contain more and more sensitive information.

We carry devices with us everywhere. The risk of loss increases the more they move around.

Loss of devices is expensive, but lost data and/or malicious network access can be dangerous.

Any device can be used as an entry point for malicious software and/or network access.

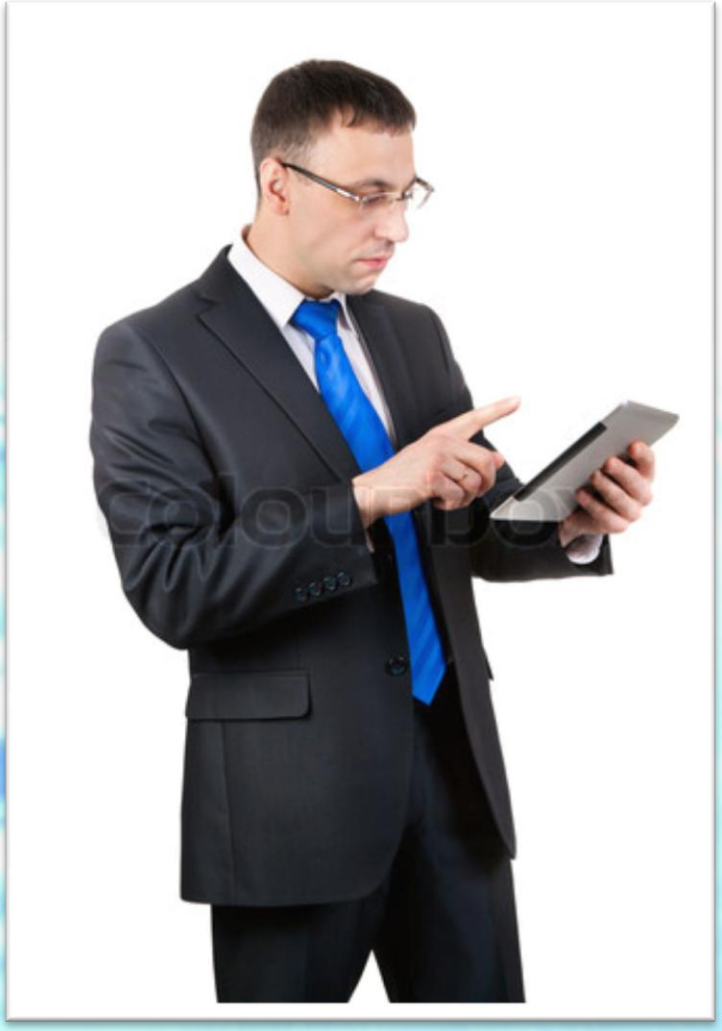
Types of Devices & Data

Smartphones
- Email & associated documents

Laptop & Tablet computers
- Email & associated documents
- System mapping (GIS data)
- Asset information
- Customer data
- SCADA interface (this is a big one!)
- Financial data
- **Remote network access** (yikes!)

Data collectors
- Customer data
- Asset information

Data Storage Devices (thumb drives)
- All kinds of data!



Security Measures

Layered approach

1. Protect the device
2. Minimize data on the device
3. Prevent access to the data and/or network connections

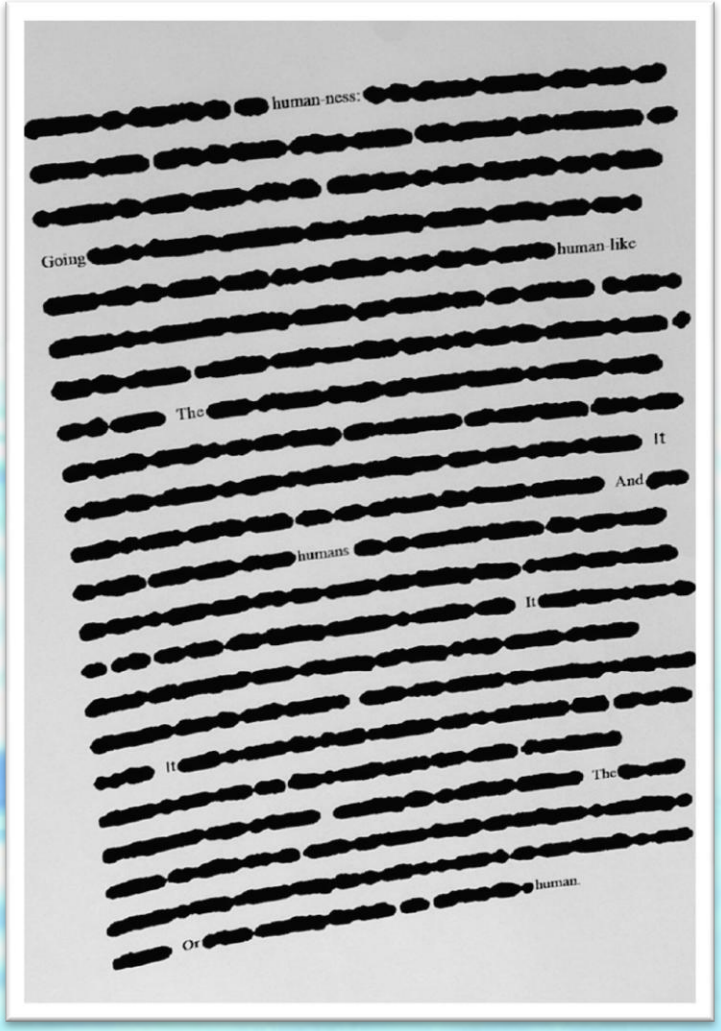
Protecting Electronic Devices

Common Sense Measures

- When they aren't locked up, keep devices in sight.
- If left in a vehicle, lock it up and leave devices out of sight.
- Don't leave devices in vehicles overnight.
- Use locking computer mounts in field crew vehicles.
- Make devices permanently identifiable.
- Include device security training with any new devices.
- Treat the device like it is a bundle of cash $$$.

Minimizing Data on Devices

- Store only data that is needed.
- Use "lean data" where it is feasible.
  - Strip attributes from GIS data
  - Remove sensitive customer data
  - Create separate maps for users
- Use cloud computing to keep data off of local hard drives.
  - Remote network access
  - Requires robust network security!



Protecting Data on Devices

- Require PIN numbers and STRONG passwords
- PIN/password lockout after multiple failed attempts
- Inactivity timeout periods
- Data encryption
- Any device can be used as an entry point to your network!

Device tracking software

Laptop Computers

- Computrace device tracking software
- Allows IT to remotely lock computer
- Devices can be unlocked if they are recovered
- Advanced capabilities include remote wiping and device locating/coordination with law enforcement

Smartphones & Tablets

- Microsoft ActiveSync
- Allows remote wiping/restoration to factory default settings
- Lookout antivirus software on smartphones & tablets

Mobile Device Security Measures

Layered approach

1. Protect the device
   - Keep them close
   - Lock them up
   - Mark them up
   - Treat them like cash $$$

2. Minimize data on the device
   - Only necessary data
   - Lean data
   - Cloud computing

3. Prevent access to the data and/or your network
   - PINs and passwords
   - Encryption
   - Inactivity timeouts
   - Remote tracking software

Contact Information

Pete Boone, PE, PLS
Engineer
Tualatin Valley Water District
503-848-3054
peteb@tvwd.org

QUESTIONS?