Overview

- BTOTS Web security features
- General security guidelines
- WiFi access & parent computers
- Desktop & laptops
- iPads & iPhones
- Browser security
- Email Security
- Physical child files
- Personally Identifiable Information (PII)
BTOTS Web Security Features

- **Data Protection**
  - Secure communication
  - Physical facility secured
  - Data encryption

- **Password Requirements**
  - 8 characters long (letters + numbers or symbols)
  - Must be changed every 3 months (cannot reuse last 3 passwords)

- **User Account**
  - Notification after 3 failed login attempts
  - Lockout after 6 failed login attempts
  - Account deactivation after 45 days of inactivity
  - Immediate deactivation when employment record ended
  - Notification on email and password change attempts
BTOTS Web Security Features CONTINUED

- **Additional Access Controls**
  - User level access controls – ability to grant access to assigned children information only
  - Application logging – log of which user has made changes and when
  - Screen & session timeout – screen fade after 5 minutes and session timeout after 15 minutes

- **Utah Department of Technology Services**
  - Vulnerability scans
  - Security updates
  - Security monitoring
BTOTS Child Information Security

FAQ sheet that can be provided to parents if they have questions.
General Security Guidelines

- **Password security**
  - Don’t share passwords with others
  - Use complex passwords
  - Don’t use a single password for every site

- **Email**
  - Ensure email password is secure
    (forgot my password feature generally relies on your email account being secure)
  - Avoid opening unknown email attachments

- **Downloads**
  - Only download applications and files from trusted sources

- Avoid using work computers for personal uses
Public and Personal WiFi Usage

- Be careful to not connect unless you are reasonably sure it is a legitimate WiFi (e.g., one that is provided by the business)
- Why is it safe to use BTOTS Web over a legitimate public or personal WiFi:
  - BTOTS requires an secure (HTTPS) connection for you to work with it
  - Communication with BTOTS Web will be encrypted from your browser all the way to the actual web server
- The following may NOT be safe on a public or personal WiFi:
  - Non-secure website (HTTP) connections
  - Email (verify with your IT staff)
- Just because the BTOTS Web connection will be secure, it doesn’t mean your computer in general will be safe. Limit the amount of additional web activity on a public WiFi connections.
Key Loggers and Phishing Attacks

- Malware and Key Loggers can record keystrokes and report them to a 3rd party
  - Do not use public or parent computers
- Phishing sends a link in an email that looks legitimate, but in reality sends the user to an illegitimate site.
  - Whenever clicking on an offsite link or email, verify that the URL is correct and it is secure.

https://btots.health.utah.gov/
WiFi Access and Parent Computers

**Public Location** (public WiFi)
- Safe to access BTOTS Web on work devices
- No public computers
- Be sensitive to visibility of screen by others

**Work Location** (work network)
- Safe to access BTOTS Web

**Home Location** (personal WiFi)
- Safe to access BTOTS Web on work devices
- No parent/personal computers

---

*Images:*
- Store designed by Martha Ormiston from The Noun Project
- Tablet designed by Luis Prado from The Noun Project
- Router designed by Pedro Lalli from The Noun Project
- Building designed by Benoit Champy from The Noun Project
- Laptop designed by The Noun Project
- Computer designed by The Noun Project
Desksots and Laptops

- Personal firewall & antivirus software
  - Enabled and automatically receives updates

- Windows updates
  - Ensure that you are getting the latest windows updates

- Password-protected
  - Secure password
  - Password-protected screen saver

- Hard drive encryption
  - Not required specifically for BTOTS Web use, but strongly recommended if you are storing any sensitive files on the laptop

- Physical security
  - Keep hardware physically safe at all times
File Encryption on Home and/or Work Computers

- TrueCrypt is a free disk encryption tool for a PC and a Mac
  - Available at [http://www.truecrypt.org/downloads](http://www.truecrypt.org/downloads)
- See tutorial showing user how to create an encrypted container (i.e., the encrypted portion of the hard disk will show up just like another hard disk when connected and unlocked via the password).
  - Tutorial available at [http://www.trucrypt.org/docs/?s=tutorial](http://www.trucrypt.org/docs/?s=tutorial)
  - Great approach for home computers as it provides a location for all work files to be placed in an encrypted "drive" and when the computer isn't being used for work purposes, it is simply not connected and is thus protected from anyone else accessing the files.
File Encryption on Home and/or Work Computers CONTINUED

- **CAUTION**: requires vigilance on the part of the user to ensure all work files are being saving to this special encrypted "drive" on the computer.
  - Files should not be saved to the desktop or “My Documents” but rather to the encrypted "drive" for all work documents.

- **CAUTION**: Truecrypt also provides mechanism for full hard disk encryption but is an involved process. Suggest that provider IT staff assist with installation.
iPads and iPhones

- UDOH iPad & iPhone security document
  - Strongly recommended if storing any sensitive files on the device
  - Step 1 minimal requirement
  - Step 2 - 4 recommended
  - Step 5, 6 are state worker specific

- Complex passcode
  - Uses a password rather than 4 numeric digits to unlock the device

- Erase data
  - Data wiped on 10 failed login attempts
Web Browser Security

- Keep your browser up-to-date
- Don’t save passwords in your browser (or require a secure master password if you do)
- Consider using an ad blocker (e.g., AdBlock Plus)
- Disable Java (but not Javascript)
- Disable ActiveX (Internet Explorer only)
Using “Master Passwords”

- Available only the Firefox browser currently.
- Requires user to enter a secure password before logins and passwords for password-protected websites will be filled in.
  - It can be applied to all saved site passwords.
- How to set a “master password” in Firefox:
  - Options > Security > Use a Master Password
- **CAUTION**: use only the built-in "Remember My Password" feature if using Firefox and have Master Password set.
- Read more about the feature at [http://kb.mozillazine.org/Master_password](http://kb.mozillazine.org/Master_password)
E-mail Security

- Do not email files or forms to parents directly
  - The parent portal uses a secure mechanism for parents to view the various child forms

- Use your official work email account
  - Don’t send sensitive information to personal email accounts (gmail, yahoo, hotmail, etc.)

- Capability for secure email isn’t the same as ensuring that email is secure
  - Some mail servers have secure connection options that are optional and not enforced

- Don’t assume that if your email is secure between co-workers it is secure if sent to someone else
  - Safest to assume email is like a postcard
Physical Child File Security

- Limit access to reports and data exports in BTOTS Web to select users
- Distribute only to those with business/clinical needs
- Store physical files in secure location such as a locked filing cabinet
- Shred all papers with sensitive information
Personally Identifiable Information (PII)

- Personally Identifiable Information (PII) includes (but is not limited to) the following:
  - Name (full or partial)
  - Shared identification numbers (e.g., SSN, driver’s license, Medicaid, CHIP, etc.)
  - Address information (street or email)
  - Telephone numbers
  - Personal characteristics (e.g., identifiable picture, x-rays, etc.)
  - Other information that can be used in combination to identify an individual

- Use the BTOTS Child ID when referring to a child in correspondence (email, support requests, etc.)
Questions/Concerns