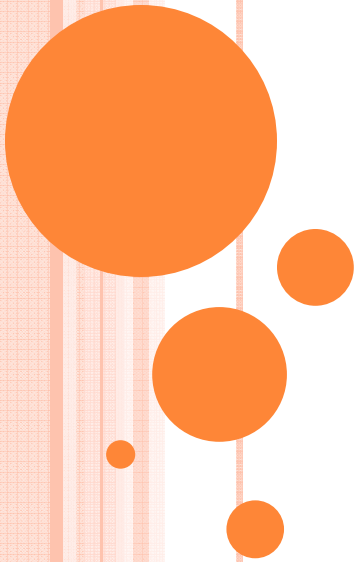


Security Training

BTOTS Web

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

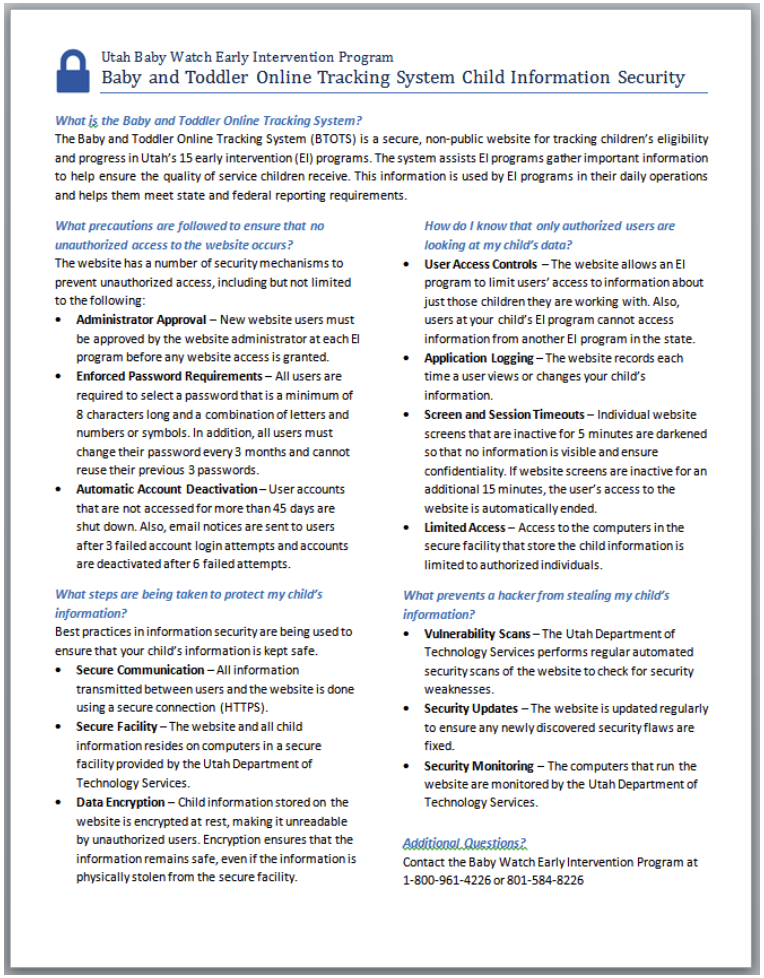
- Data Protection
  - Secure communication
  - Physical facility secured
  - Data encryption
- Password Requirements
  - 8 characters long (letters + numbers or symbols)
  - Must be changed every 3 months (cannot reuse last 3 passwords)
- User Account
  - Notification after 3 failed login attempts
  - 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.



Utah Baby Watch Early Intervention Program

Baby and Toddler Online Tracking System Child Information Security

What is the Baby and Toddler Online Tracking System?

The Baby and Toddler Online Tracking System (BTOTS) is a secure, non-public website for tracking children's eligibility and progress in Utah's 15 early intervention (EI) programs. The system assists EI programs gather important information to help ensure the quality of service children receive. This information is used by EI programs in their daily operations and helps them meet state and federal reporting requirements.

What precautions are followed to ensure that no unauthorized access to the website occurs?

The website has a number of security mechanisms to prevent unauthorized access, including but not limited to the following:

- **Administrator Approval** – New website users must be approved by the website administrator at each EI program before any website access is granted.
- **Enforced Password Requirements** – All users are required to select a password that is a minimum of 8 characters long and a combination of letters and numbers or symbols. In addition, all users must change their password every 3 months and cannot reuse their previous 3 passwords.
- **Automatic Account Deactivation** – User accounts that are not accessed for more than 45 days are shut down. Also, email notices are sent to users after 3 failed account login attempts and accounts are deactivated after 6 failed attempts.

What steps are being taken to protect my child's information?

Best practices in information security are being used to ensure that your child's information is kept safe.

- **Secure Communication** – All information transmitted between users and the website is done using a secure connection (HTTPS).
- **Secure Facility** – The website and all child information resides on computers in a secure facility provided by the Utah Department of Technology Services.
- **Data Encryption** – Child information stored on the website is encrypted at rest, making it unreadable by unauthorized users. Encryption ensures that the information remains safe, even if the information is physically stolen from the secure facility.

How do I know that only authorized users are looking at my child's data?

- **User Access Controls** – The website allows an EI program to limit users' access to information about just those children they are working with. Also, users at your child's EI program cannot access information from another EI program in the state.
- **Application Logging** – The website records each time a user views or changes your child's information.
- **Screen and Session Timeouts** – Individual website screens that are inactive for 5 minutes are darkened so that no information is visible and ensure confidentiality. If website screens are inactive for an additional 15 minutes, the user's access to the website is automatically ended.
- **Limited Access** – Access to the computers in the secure facility that store the child information is limited to authorized individuals.

What prevents a hacker from stealing my child's information?

- **Vulnerability Scans** – The Utah Department of Technology Services performs regular automated security scans of the website to check for security weaknesses.
- **Security Updates** – The website is updated regularly to ensure any newly discovered security flaws are fixed.
- **Security Monitoring** – The computers that run the website are monitored by the Utah Department of Technology Services.

Additional Questions?

Contact the Baby Watch Early Intervention Program at 1-800-961-4226 or 801-584-8226

General Security Guidelines

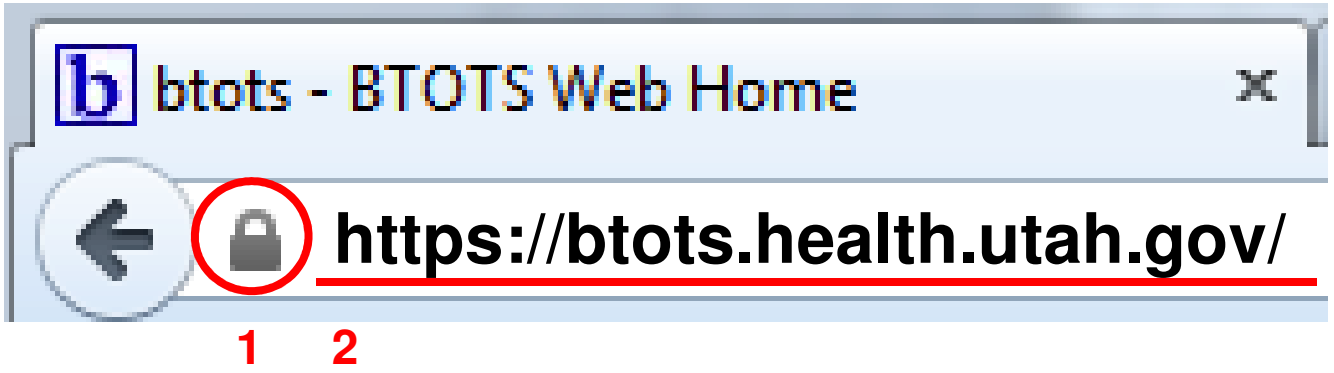
- Password security
  - Don’t share passwords with others
  - Use complex passwords
  - Don’t use a single password for every site
- Email
  - Ensure email password is secure (forgot my password feature generally relies on your email account being secure)
  - Avoid opening unknown email attachments
- 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

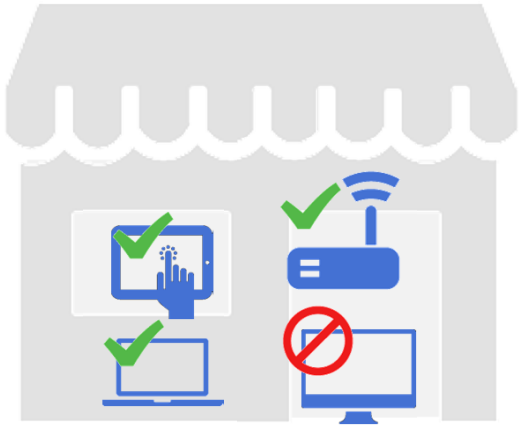
- Malware and Key Loggers can record keystrokes and report them to a 3rd party
  - Do not use public or parent computers
- Phishing sends a link in an email that looks legitimate, but in reality sends the user to an illegitimate site.
  - Whenever clicking on an offsite link or email, verify that the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



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

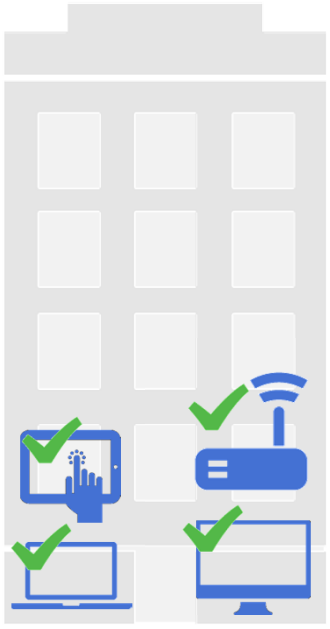


Store designed by Martha Ormiston from The Noun Project

Tablet designed by Luis Prado from The Noun Project

Work Location
(work network)

- Safe to access BTOTS Web



Router designed by Pedro Lalli from The Noun Project

Building designed by Benoit Champy from The Noun Project

Home Location
(personal WiFi)

- Safe to access BTOTS Web on work devices
- No parent/personal computers

Laptop from The Noun Project

Computer from The Noun Project

Desktops 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

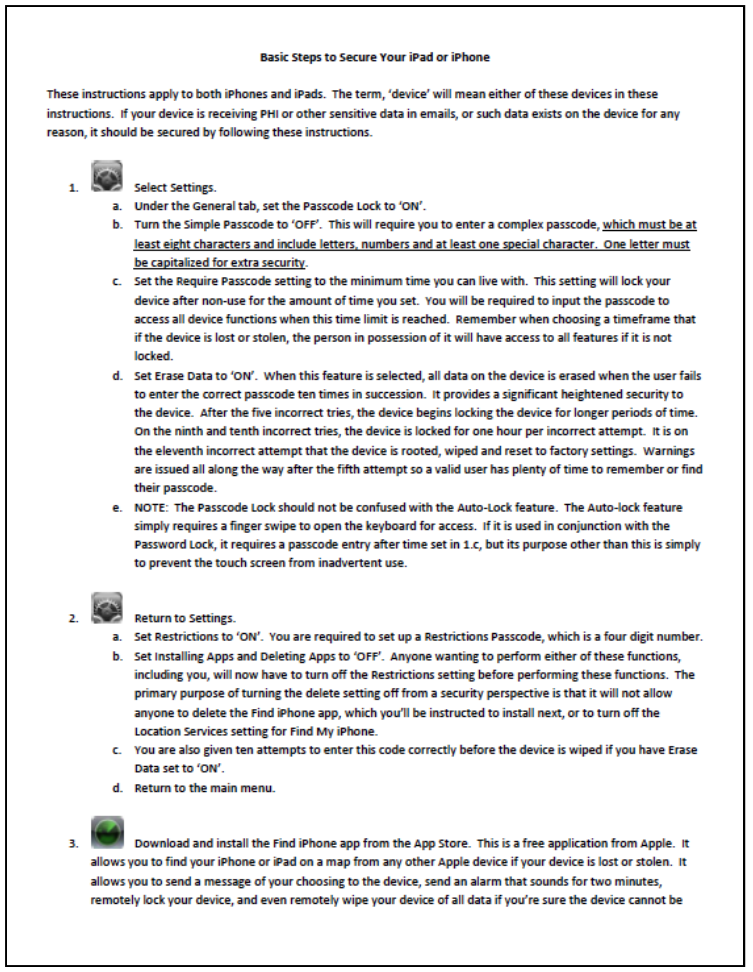
- TrueCrypt is a free disk encryption tool for a PC and a Mac
  - Available at http://www.truecrypt.org/downloads
- See tutorial showing user how to create an encrypted container (i.e., the encrypted portion of the hard disk will show up just like another hard disk when connected and unlocked via the password).
  - Tutorial available at http://www.trucrypt.org/docs/?s=tutorial
  - 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



Basic Steps to Secure Your iPad or iPhone

These instructions apply to both iPhones and iPads. The term, 'device' will mean either of these devices in these instructions. If your device is receiving PHI or other sensitive data in emails, or such data exists on the device for any reason, it should be secured by following these instructions.

1. Select Settings.
   a. Under the General tab, set the Passcode Lock to 'ON'.
   b. Turn the Simple Passcode to 'OFF'. This will require you to enter a complex passcode, which must be at least eight characters and include letters, numbers and at least one special character. One letter must be capitalized for extra security.
   c. Set the Require Passcode setting to the minimum time you can live with. This setting will lock your device after non-use for the amount of time you set. You will be required to input the passcode to access all device functions when this time limit is reached. Remember when choosing a timeframe that if the device is lost or stolen, the person in possession of it will have access to all features if it is not locked.
   d. Set Erase Data to 'ON'. When this feature is selected, all data on the device is erased when the user fails to enter the correct passcode ten times in succession. It provides a significant heightened security to the device. After the five incorrect tries, the device begins locking the device for longer periods of time. On the ninth and tenth incorrect tries, the device is locked for one hour per incorrect attempt. It is on the eleventh incorrect attempt that the device is rooted, wiped and reset to factory settings. Warnings are issued all along the way after the fifth attempt so a valid user has plenty of time to remember or find their passcode.
   e. NOTE: The Passcode Lock should not be confused with the Auto-Lock feature. The Auto-lock feature simply requires a finger swipe to open the keyboard for access. If it is used in conjunction with the Password Lock, it requires a passcode entry after time set in 1.c, but its purpose other than this is simply to prevent the touch screen from inadvertent use.

2. Return to Settings.
   a. Set Restrictions to 'ON'. You are required to set up a Restrictions Passcode, which is a four digit number.
   b. Set Installing Apps and Deleting Apps to 'OFF'. Anyone wanting to perform either of these functions, including you, will now have to turn off the Restrictions setting before performing these functions. The primary purpose of turning the delete setting off from a security perspective is that it will not allow anyone to delete the Find iPhone app, which you'll be instructed to install next, or to turn off the Location Services setting for Find My iPhone.
   c. You are also given ten attempts to enter this code correctly before the device is wiped if you have Erase Data set to 'ON'.
   d. Return to the main menu.

3. Download and install the Find iPhone app from the App Store. This is a free application from Apple. It allows you to find your iPhone or iPad on a map from any other Apple device if your device is lost or stolen. It allows you to send a message of your choosing to the device, send an alarm that sounds for two minutes, remotely lock your device, and even remotely wipe your device of all data if you're sure the device cannot be

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

E-mail Security

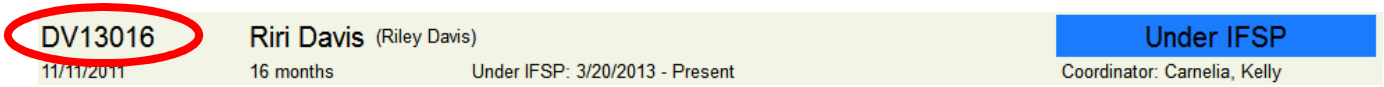
- Do not email files or forms to parents directly
  - The parent portal uses a secure mechanism for parents to view the various child forms
- Use your official work email account
  - Don't send sensitive information to personal email accounts (gmail, yahoo, hotmail, etc.)
- Capability for secure email 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