

Security Awareness Training

BUG MEETING - JAN 9, 2020





" WHEN IT COMES DOWN TO IT, JIM,
SECURITY IS A PERSONAL RESPONSIBILITY. "

[J Klossner \(http://www.jklossner.com\)](http://www.jklossner.com)

Overview

BTOTS security features

General security guidelines

Wi-Fi access & parent computers

Desktop & laptops

Tablets & phones

Browser security

Email security

Physical child files

Personally Identifiable Information (PII)

BTOTS 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

Security Features (cont...)

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 35 minutes
- User Account Access Report – used to periodically review user's access

User Account Summary

The lists below display administrator accounts, accounts awaiting access, and those with ended employments that should be deactivated. Click the "View All User Accounts" button to the right to display all user accounts in the system.

[View All User Accounts](#)


[View User Access Report](#)

Utah Department of Technology Services

- Vulnerability scans
- Security updates
- Security monitoring

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 Wi-Fi Usage

Be careful to not connect unless you are reasonably sure it is a legitimate Wi-Fi (e.g., one that is provided by the business)

Why is it safe to use BTOTS over a legitimate public or personal Wi-Fi:

- BTOTS requires an secure (HTTPS) connection for you to work with it
- Communication with BTOTS 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 Wi-Fi:

- Non-secure website (HTTP) connections
- Email (verify with your IT staff)

Just because the BTOTS 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 Wi-Fi connections. Ensure that your windows firewall is turned on and set to public connection.

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.

- Before clicking on an offsite link or email, verify that the URL is correct and it is secure.

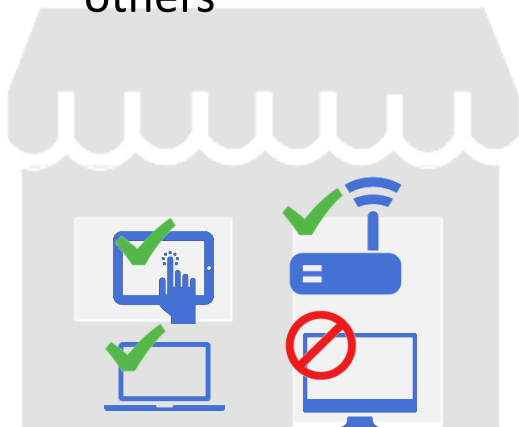


Wi-Fi Access & Parent Computers

Public Location

(public Wi-Fi)

- Safe to access BTOTS on work devices
- No public computers
- Be sensitive to visibility of screen by others



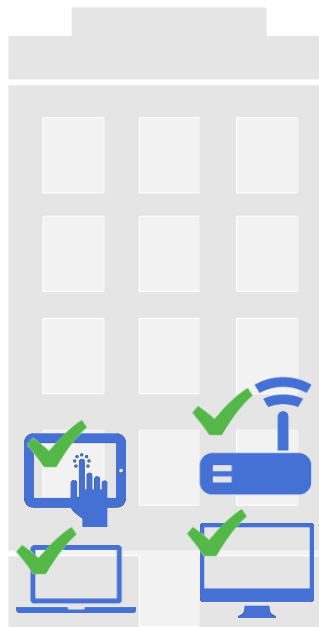
Store designed by [Martha Ormiston from The Noun Project](#)

Tablet designed by [Luis Prado from The Noun Project](#)

Work Location

(work network)

- Safe to access BTOTS



Router designed by [Pedro Lalli from The Noun Project](#)

Building designed by [Benoit Champy from The Noun Project](#)

Home Location

(personal Wi-Fi)

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



Laptop from [The Noun Project](#)

Computer from [The Noun Project](#)

Desktop & 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 with reasonable timeout

Hard drive encryption

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

Physical security

- Keep hardware physically safe at all times

Tablets & Phones

Complex passcode

- Avoid using a 4 digit pin (use biometrics, password, or at least a 6 digit pin)

Keep software updated

Lock after inactivity

Encrypt your device

Avoid jailbreaking

Authorized App Stores

- Use only authorized App stores for obtaining applications

Data wipe feature

- Data wiped on 10 failed login attempts or remote initiated wipe

Web Browser Security

Use a current browser: Firefox, Chrome, Safari, Edge
(i.e. **not** Internet Explorer)

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 and privacy blocker
(e.g., Adblock Plus, Privacy Badger)

Email Security

Do not email files or forms to parents directly unless using a secure email system.

- 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 to select users

Consider using the “Child ID” instead of “Child Name” option for reports.

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

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.)

FT199546	Trevor Alehill		Pending IFSP
4/4/2019	9 mo. (8 mo. adj)	Referred: 6/17/2019; 10/28/2019	Coordinator: Tantalón , Emma

Additional Security Measures

Additional upcoming security measures in BTOTS

- Improved process of reporting on child views by users (e.g., ledger of child data access)
- Archiving children that have been deactivated more than 5 years (Provider administrators will still be able to view older accounts)

Submit security suggestions via support tickets

- Please make us aware of security concerns related to the BTOTS website

Questions/Concerns
