Report a Security Incident / Recover from a Device Theft

patricia falcon - 2023-09-05 - Comments (0) - Physical Security

If you become aware of an event that could result in a breach of personally identifiable information (PII), it is critical that you immediately report any information or network security incident to the **OIT Service Center** and follow these recommended procedures.

For a Lost or Stolen Electronic Media or Computing Device

- **Wipe devices:** If it's possible, you should remotely wipe your device to prevent any contents from being accessed by another.
    - **Brown-owned laptops and tablets:** Contact your ITSC (IT Support Consultant) or DCC (Departmental Computing Coordinator) for assistance.
    - **Brown-owned phones:** Notify the Telecommunications Office immediately (**telecom@brown.edu**, 401-863-2007). Telecom will suspend voice services and issue a remote wipe of the device, if applicable.
    - **Personally-owned laptops, tablets and phones:** If the device has wipe functionality, activate it. For phones, you should also notify your service provider to suspend your service.
- **Track the device:** If the device has third-party tracking software installed, contact the company, or if applicable, activate its tracking function.
- **File a report with law enforcement:** Contact the **Department of Public Safety** (401-863-3103) if the loss occurred on campus, or to local police, to report lost or stolen electronic media or a computing device, whether it is Brown-issued or personally owned.
- **High risk information:** If the lost or stolen device was used to store information with **Level 2 or 3 risk**, please include this in your report to the OIT Service Center. Note that when the Information Security Group follow up, you will be asked to complete the **Missing, Lost or Stolen Device online form** . ISG will then work with you to determine the next steps, and whether the event requires notification.

For Device or Information Intrusion

- If you suspect that someone has broken into your device, please disconnect it from the network ASAP. If it is Brown-owned, contact your ITSC or DCC; if personally owned, reach out to the OIT Service Center.
- Include the following details about the incident: when and where it occurred, device specifics (such as OS, type, owner), any accounts that may have been impacted.

They will investigate the incident and help you recover your system.

- If an account may have been compromised, change your password in **myaccount.brown**. If your Gmail account was compromised, follow the other account recovery steps outlined in **Secure a Compromised Gmail Account**.