

## Reporting a Security Incident

patricia falcon - 2024-08-13 - Comments (0) - Physical Security

If you are aware of a security incident or have been successfully targeted by a malicious threat actor, it is crucial to report the incident immediately. A security incident can take many forms, including but not limited to:

- **Device theft:** The loss or theft of a university device containing sensitive information.
- **Phishing, job scams, financial fraud/extortion, loss of PII:** Incidents where fraudulent schemes have led to monetary losses or the inadvertent disclosure of sensitive personally identifiable information (PII) such as passwords, banking information, or other confidential data .
- **Network intrusion:** Unauthorized access to Brown University's network, including any connected devices
- **Viruses, malware or ransomware attacks:** Incidents where malicious software is used to disrupt use of a Brown device or demand a ransom for the return of access to your files or systems.

In the event of a security incident, you must submit a security incident ticket to the Office of Information Technology (OIT). To create a ticket, you can either **email** [help@brown.edu](mailto:help@brown.edu), use the **Submit a Ticket** form, or reach out by **phone**: 401-863-4357. To ensure a **quick** response, we recommend reaching out by **phone**.

While it is important to report suspicious emails and phishing attempts, please note that these should be [reported via the Phish Alert button](#) in your Gmail inbox or directed to the [Phish Bowl](#) at [phishbowl@brown.edu](mailto:phishbowl@brown.edu). The Phish Bowl is a valuable tool for making OIT aware of potential phishing messages. However, it is not an incident response tool and is not intended for reporting active security incidents.

**If you have fallen victim to a phishing scam or any other form of fraud, and it has resulted in losses or exposure of sensitive information, it is essential to report it as a security incident through the appropriate channels mentioned above.**

When in doubt, reach out! Members of our community should never hesitate to report a potential security incident. If you suspect a security incident or data compromise, report it immediately. This isn't just best practice - it's the mission of OIT. Brown is committed to ensuring the safety and security of our community's data and information systems, and our community members are a critical component of that mission and culture.