Learn About Safe Computing at Brown

Stephanie Obodda - 2023-05-12 - Comments (0) - General Security

New to the Brown computing environment? Then you may find answers to your questions in this list of common inquiries.

Q: What does Brown do to protect me from email viruses or when I'm on the network?

A: Brown's uses Google Apps for Education for its email service. Gmail automatically scans every attachment for viruses when an attachment is delivered to you, and again each time you open the message. See the Gmail document **Anti-virus scanning attachments** for details.

The Office of Information Technology (OIT) uses multiple methods to protect the Brown network. This includes monitoring for malicious behavior and external intruders, scanning hosts on the network for suspicious anomalies, and blocking harmful traffic. For example, OIT will take action to quarantine devices that impose an exceptional load on a campus service or disrupt centrally-provided services, or will restrict traffic that is known to cause damage to the network or consume too much network capacity, such as file-sharing traffic. See the **Network Connection Policy** for security standards, your responsibilities, and protection of the network.

By connecting to the Brown's network, you agree not to cause any of the behaviors listed above which are in violation of policy and you also understand that any computer that does cause problems will be removed from the network until it is once again compliant.

Q: I already have anti-virus software on my computer. Why should I install Brown's version?
A: Because Brown's software is specially configured for Brown's environment to provide optimum protection, and it's free to any Brown University registered student. You can download a copy from the **Software Catalog**.

Q: When I activated my Brown account, I had to agree to a couple of policies before I could connect. Do they live someplace else in case I want to go back and see what I agreed to?
A: Yes. They reside on the **OIT Policies** page.

Q: Does someone monitor what I send in email or do on the Internet?
A: While the University does not generally monitor or limit content of information transmitted on the campus network, it does reserve the right to access and review such information under rare but certain conditions. These include: investigating performance deviations and system problems (with reasonable cause), determining if an individual is in violation of this policy, or, as may be necessary, to ensure that Brown is not subject to claims of institutional misconduct. More details can be found in Brown's **Acceptable Use of IT Resources Policy.**

Q: I think I might be infected with malware or answered a phishing email? What can I do?
A: Contact the Phish Bowl at phishbowl@brown.edu with questions and visit it at brown.edu/go/phishbowl for a compendium of reported phishing emails.

Q: There's lots of talk about "strong passwords"? What's considered strong?
A: The basic rule of thumb is "something hard for someone to guess but easy for you to remember". Details on Brown's minimum requirements and how to create a good password can be found in the document **Create a Strong Password.**

Q: I've heard that there are wireless access points all over campus. How can I get connected?
A: You can access the wireless at **http://wifi.brown.edu.** See **Connect to Brown's**

Wireless Network for more details.

Q: Can I trust a wireless connection for confidential communications or downloads?

A: Brown's wireless network is a secured one, preventing other wireless users from collecting private data from you. When off-campus, avoid public wi-fi and protect yourself by using **Brown's VPN (Virtual Private Network).** VPN (**http://vpn.brown.edu**) provides a secure "tunnel" that will also allow you to use most Brown applications.

For general questions about information security or to report a computing security incident, contact **ISG@brown.edu.** Contact the **IT Service Center** for other computing concerns.