



Cybersecurity Awareness



Be cybersecurity aware

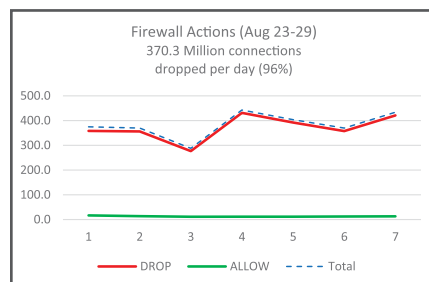
The University is connected to the Internet. People on campus enjoy access to the web, media, social services, email and chat, etc. Internet access is a two-way street, however, and people and devices on the Internet can also access the campus. This allows students and staff to reach services like UWinsite Student and Blackboard from their homes and mobiles. It also allows anyone else to connect as well, and not everyone on the Internet has good intentions.

Internet access is a two-way street; people and devices on the Internet can also access the campus.

The accounts, information and research, and computing resources at the University are of value to hackers, spies and criminals. They look to hack into accounts in order to gain access to research, to send phishing messages and spam, or to take over computers for cryptomining and botnets. This note provides some information on hacker activity on campus and where you can find information to protect yourself.

A Hostile Internet

Unfortunately, the Internet can be a hostile environment. Computers are good at repetition, and this allows bad actors to automate attacks on their victims. These attacks include trying to break into accounts and scanning to find vulnerabilities and other weaknesses to exploit. The front line of defence for campus against these robotic attacks is a firewall. A firewall allows desired connections and drops undesired or suspect traffic.



The graph above shows that our firewall drops over 96% of connections from the Internet as being invalid or prohibited connection attempts.

Multiple Threat Vectors

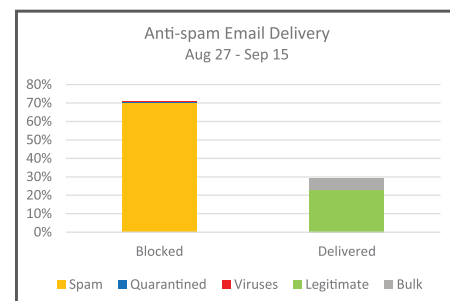
The security of campus information and computing resources is regularly threatened by a variety of factors using a variety of techniques and attacks, such as:

- Phishing and spear-phishing attacks
- Malware and ransomware
- Compromised accounts
- Malicious apps on mobile
- Theft and loss of equipment

The important thing to know is that there is a mature, organized industry that is seeking access, information and resources. Computer users on campus need to stay aware and report anything unusual to IT Services so it can be checked.

Phishing and Spam

Email is a critical communication tool, but it can be abused. Everyone has seen spam emails and phishing attempts in their Inboxes. Phishing and its more targeted cousin, spear phishing, are attempts to fool recipients of a message to reveal information (such as their username and password) or perform an action on behalf of the phisher. What people don't know is that the spam and phishing attempts that reach their mailbox are only the tip of the iceberg. The campus has multiple anti-spam systems in place that stop the vast majority of unwanted email before it even reaches the recipient.



In the last month, more than 70 percent of emails sent to the campus were blocked by our anti-spam systems.



cybersecurity
awareness
UNIVERSITY OF WINDSOR

We're here to help!

IT Services is happy to answer questions about cybersecurity on campus: **ext. 4440** or open a ticket for service here: uwindsor.ca/itshelp. More information on cybersecurity issues facing campus: uwindsor.ca/cybersecurity