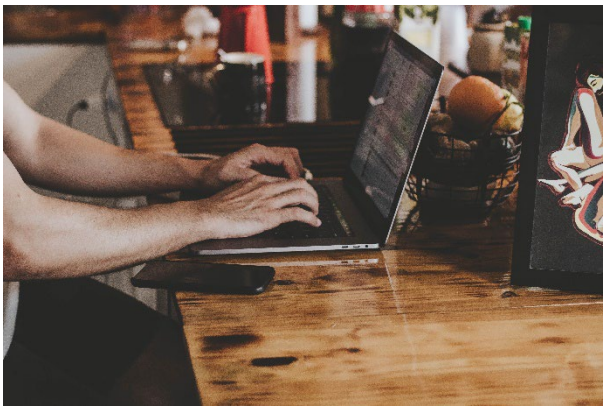
Threat of Malicious URLs



Cybersecurity threats are on the rise, and one of the most common ways cybercriminals infiltrate networks is through malicious URLs. These links direct users to websites containing malware, which can infect computers, steal sensitive data, or trick users into revealing personal information, such as passwords and credit card numbers. It's essential to be aware of the dangers of malicious URLs and how to protect yourself and DCH.

Here are some steps you can take:

- **Avoid clicking on suspicious links**: If you receive an email or message containing a link from an unknown sender, don't click on it. Instead, hover over the link, and if it looks even remotely suspicious, report it to the Cybersecurity team.
- **Check URLs carefully:** Before clicking on any link, examine the URL to ensure it is legitimate. Misspellings can be a tell-tale sign that it may be fake. Also, utilizing the Talos Intelligence Reputation Center website can help determine whether a URL is safe. It can detect malicious URLs and warn you before you click on them, which can help protect your computer from malware and other security threats.
- **Stay informed:** Protecting DCH is a team sport, and knowledge is power! There are many free tools that you can use to stay up to date on the latest cybersecurity threats and trends – for example, The Hacker News, Security Week, or Threat Post. Because cyber-attacks are prevalent today, watching the news or cybersecurity-themed YouTube channels such as CyberNews is also an easy way to stay informed.

If you think your work computer is infected with a virus or are unsure about a URL, immediately contact the DCH Helpdesk at hrhelp@dch.ga.gov, call (404) 657-7171), or reach out to the Cybersecurity team at mdchois@dch.ga.gov.