Cloud Destinations
Embrace Cloud Multiverse

Safe Internet Browsing

Overview

The landscape for cyber threats (e.g., phishing, viruses, malware, ransomware, etc.) is constantly evolving. While the Office of the Chief Information Officer (OCIO) uses industry standard security technologies to monitor, detect and defend against these threats; employees also play an important role.

Technology and the Internet are increasingly used in the workplace and it is important for allemployees to be diligent in their daily activities. Employees should consider using safe web browsing best practices at all times to help prevent cyber-attacks to the Cloud Destintions Network and its information assets.

Best Practices

Always On, Always Connected. Always leave your work computer powered on and connected to the Cloud Destinations network to help ensure critical security updates are applied.

Verify the authenticity of an unknown website by:

- Typing the website's name into a search engine (e.g., Google) and reviewing the results.

- Manually typing URLs in the browser's address bar rather than clicking on links in email. This will help ensure you are visiting a legitimate website and not amalicious or fake website (e.g., www.account.google.com would be the correct URL for the official website whereas www.google.account.com would be an URL for a malicious or fake website).

- URLs that include hyphens, numbers, spelling mistakes and the @ symbol in place of regular characters should be considered suspicious.

- Look for “Secure” or a padlock icon in the browser’s address bar. Click the padlockicon and view the security information ensuring the URL displayed is the same URLyou are visiting.

- Review the content of the website. Are there spelling and grammar mistakes on important web pages? Is the overall website experience haphazard versus streamlined and polished? Is there an overabundance of advertisements? If you answer yes to any of these questions, it should be an immediate red flag.

- Review the website’s contact page. If a website does not have a contact page listedanywhere, it should be an immediate red flag.

Be careful what you post or download.

Clear cached data, which is memory stored in your web browser or on your mobile device containing sensitive information such as personal data, passwords, cookies, browsing data, etc.

Only provide confidential information requested on a website when you have verified the website’s authenticity and the website address begins with ‘https’; the ‘s’ stands for secure.

Never disclose your Cloud Destinations-issued credentials (e.g., username and

password).Never use your Cloud Destinations-issued email address for personal use.

Do not use the same security questions and passwords for your Cloud Destinations employeeactivities and personal activities.

When searching for information on the Internet using your Cloud Destinations-issued computer, click on search results that have search protection annotation (e.g., green check mark to theright of the search result.

Bookmark websites you trust and visit regularly.