

# Internet Safety Tips for Employees

Topic	Key Themes	Expected Benefits
Safe Internet Habits	<ul style="list-style-type: none"> <li>• <b>Click Smart</b> – before clicking on a link, hover your mouse over the link and check the dialogue window that appears. Make sure the link in the window matches the link you are about to click.</li> <li>• <b>Be Wary of Popups</b> – some popups contain viruses which can be triggered by clicks</li> <li>• <b>Avoid Suspicious Content</b> – avoid websites that contain questionable content such as illegal downloads, sexual content, free prizes, etc.</li> <li>• <b>Don't Enter Information</b> – never enter any information into online forms unless they're from a trusted site. Sites may phish your personal information using fake forms (e.g. registration forms, subscription opt-ins)</li> </ul>	<p>Employees who consistently display safe internet browsing habits <b>mitigate the risk to company assets, personal information, and software/hardware.</b></p>
Social Media	<ul style="list-style-type: none"> <li>• <b>Selective Sharing</b> – Always be cautious of what you're sharing online. Post under the assumption that it will become free for public viewing, and may never be removed from the internet</li> <li>• <b>Understand Privacy Settings</b> – Familiarize yourself with your social media platform's security settings. They exist to help you control what you post and to manage your online experience</li> <li>• <b>Keep Personal Things Personal</b> – Understand what content is personal, and what impacts your professional life. When posting, realize that any mention of your employer makes you a representative of your organization.</li> </ul>	<p>Employees will know <b>what's appropriate to post, and how their posts impact</b> their workplace, and their careers.</p>
Email Scams	<ul style="list-style-type: none"> <li>• <b>Unsolicited emails</b> – any unsolicited emails should raise a red flag immediately.</li> <li>• <b>Think Before You Download</b> – Read, Read, Read! Always check the entire email before you download any attachments. Attachments can contain viruses and malware.</li> <li>• <b>Take Action</b> – Once you've identified a suspicious email, make sure employees know what actions to take, and who to report the threat to.</li> </ul>	<p>Employees will understand how to <b>identify and report suspicious email</b> activity.</p>

