Cybersecurity at Work Picture This – French

Cette image montre un employé de bureau confronté à une tentative d’hameçonnage à son insu, avec un message en gras « ACTION URGENTE REQUISE » et un bouton rouge suspect l’invitant à « cliquer pour vérifier son compte maintenant ». Il s’agit d’une menace classique en matière de cybersécurité, souvent utilisée pour inciter les employés à cliquer sur des liens malveillants qui conduisent à des violations de données, au vol d’identifiants ou à des attaques par ransomware.

Tous les employés doivent suivre régulièrement des formations de sensibilisation à la cybersécurité, notamment sur l’identification des e-mails de phishing, des fenêtres

contextuelles urgentes, des liens suspects et des tactiques d’ingénierie sociale. Mettez en place des protocoles informatiques clairs pour signaler les messages suspects. Encouragez l’utilisation de canaux vérifiés pour confirmer l’authenticité avant de cliquer. Les employeurs doivent déployer des filtres de messagerie, une protection des terminaux et une authentification multifactorielle afin de réduire les risques. La cybersécurité est la responsabilité de tous : un seul clic peut compromettre l’ensemble de l’organisation.