CYBER SECURITY AWARENESS MONTH

MAKE YOUR WORK DEVICES WORK FOR YOU

A GUIDE FOR EMPLOYEES

In some ways, our workplace devices are our favourite coworkers. But if we're not careful, they can also expose us to serious threats.

Here are some tips on how you can safely use your work devices, no matter where work is.

WATCH OUT FOR SOCIAL ENGINEERS

85% of organizations are the target of social engineering attacks, like phishing[i]

CONFIRM THE IDENTITY OF ANYONE MAKING UNUSUAL EMAIL OR TEXT REQUESTS

BE CAREFUL GIVING OUT INFO ABOUT YOUR ORGANIZATION OR ITS EMPLOYEES

REPORT ANY SUSPICIOUS ACTIVITY TO YOUR SUPERVISOR ASAP

KEEP A PROFESSIONAL RELATIONSHIP WITH YOUR PHONE

Mobile devices can be a cyber criminal's window into your organization.

DON'T LEAVE YOUR PHONE UNLOCKED OR UNATTENDED

KEEP SENSITIVE WORK INFORMATION OFF YOUR PERSONAL DEVICES

FOLLOW YOUR ORGANIZATION'S SOCIAL MEDIA POLICY

ONLINE RISKS ARE JUST A CLICK AWAY

Malware attacks cost organizations an average of **$3.4 million** each year.[i]

LOCK YOUR COMPUTER WHEN YOU LEAVE YOUR DESK

BACK UP YOUR FILES TO AN EXTERNAL HARD DRIVE OR CLOUD OFTEN

CONTACT IT BEFORE INSTALLING ANY NEW SOFTWARE

CONNECT SAFELY, NO MATTER WHERE YOU ARE

The internet makes your job easier – but it can also put you at risk.

USE A VPN WHEN WORKING REMOTELY

NEVER SHARE YOUR ORGANIZATION'S WI-FI PASSWORD

NEVER DISABLE FIREWALLS OR ANTI-VIRUS APPS

AND ABOVE ALL ELSE, FOLLOW YOUR ORGANIZATION'S CYBER SECURITY POLICY.

IF YOU HAVE ANY QUESTIONS ABOUT STAYING CYBER SAFE AT WORK, CONTACT YOUR IT DEPARTMENT OR VISIT

GETCYBERSAFE.CA

[i] THE COST OF CYBERCRIME, ACCENTURE SECURITY, 2019