**CYBER READINESS**
INSTITUTE

# Ho Ho, Oh No!

## Cyber Readiness Tips for Retailers During the Holidays

The holiday shopping season is getting into full swing, but like so many regular activities, **shopping is different this year because of the COVID-19 pandemic.**

More people are shopping online than ever before. According to McKinsey, between 30 and 60 per cent of consumers across the globe expect to move their shopping online during the holidays. Retailers have had to respond by making it easier for consumers to buy online and establish new ways for buyers to receive their purchases. For many retailers, this reality has led to contracting delivery services, which means retailers are sharing customer information with third parties. The entire buying process, from start to finish, relies increasingly on transferring information between you and your customers, who are using computers and smartphones. Today's advanced technology has made it possible for retailers — even small ones — to rapidly shift more of their business to a digital platform. That's great news in addressing the business challenges that have increased because of the pandemic.

The bad news is that criminals have also made the move to the digital world. Cyber criminals know that more people are shopping online and that retailers are collecting and sharing more valuable information about their customers — including credit card numbers, addresses, and photo identification for curbside pick-up. There has been an enormous increase in email and text phishing attacks — attempts to fool you into clicking on a link or sending information — and ransomware attacks where criminals hold your computer system and data hostage until they receive payment. The FBI has reported a 400 per cent increase in cyber attack complaints from pre-COVID-19 times. While Interpol has tracked an "alarming rate of cyberattacks" aimed at business of all sizes, governments, and critical infrastructure during the pandemic.

We know that it's a busy time of year and that you're focused on serving your customers. We realize that you may be bringing on seasonal workers or starting to work with new delivery services and partners. But the criminals know this too, and they are counting on you being distracted and neglecting cyber readiness. Unfortunately, 60% of small businesses go out of business within 6 months after a serious cyber incident, according to the National Cyber Security Alliance.

You might think that your business is too small to be a target, but you may be an easy gateway to a desired larger target.
Here are some tips to help you be cyber ready in the holiday shopping season:

## Do

- ✓ Immediately update your passwords to 15-characters — using a passphrase can make it easier to remember (e.g. lyric from a song, line from a book)

- ✓ Turn on auto-updates for all software

- ✓ Use multi-factor authentication any time it is available

- ✓ Make sure that your computers and data are backed-up on a separate network and test that back-up regularly

- ✓ Have clear cyber policies in place that are communicated to all employees

- ✓ Train employees on how to receive and process online orders safely and securely

## Don't

- ✗ Don't click on links and never provide financial information via email

- ✗ Don't share your passwords or log-in credentials

- ✗ Don't leave any computers unattended and/or unlocked

- ✗ Don't assume that your third parties are cyber ready (e.g., delivery services, payment processors, small suppliers)

## Remember that human behavior is critical in preventing a cyber attack.

Ensure all your employees and seasonal workers are trained in your cybersecurity policies, that they know the importance of cybersecurity and their role in it. Help them develop good cyber readiness habits. For more details, please register for the Cyber Readiness Program and look at our **other guides** to develop good cyber readiness habits.

### About the Cyber Readiness Institute

The Cyber Readiness Institute is a non-profit initiative that convenes business leaders from across sectors and geographic regions to share resources and knowledge that inform the development of free cybersecurity tools for small and medium-sized enterprises (SMEs). Explore the building blocks of good cybersecurity with our Starter Kit or create a cyber readiness culture in your organization with the self-guided, online Cyber Readiness Program. Our Remote Work Resources and Hybrid Workplace Guides offer timely tips for addressing the evolving cyber challenges of today. To find out more, visit **www.BeCyberReady.com**.