JONESDESLAURIERS
INSURANCE MANAGEMENT INC.

NAVACORD®

BE CYBER SMART. BE CYBER SAFE.

Local Touch. National Strength.™

JONESDESLAURIERS INSURANCE MANAGEMENT INC. | NAVACORD®

The outbreak of COVID-19 has caused significant disruption to businesses everywhere. Of course, while everyone works to ensure key business functions remain operational and that employees and families everywhere are safe, there is another set of individuals working just as hard to disrupt our efforts: *cyber criminals*.

Employees are your **first line of defense** against cyber attacks and scams.

Be vigilant—watch what you open, click on, or download.

Review the tips throughout the document and be cyber smart, so you can be cyber safe.

Almost All Phishing Attacks Can Be Broadly Divided Into **Two Categories:**

1. Tricking users to pass on sensitive information via spoofed sites

This method creates compelling communication messages that entice the user into visiting third-party, data harvesting sites.

2. Getting the user to install malware through a click in a communication

In this method, the fraudster entices the user to click on a download link that in turn installs malware.

Red Flags That Will Help You Spot **Phishing Scams & Attacks:**

1. Incorrect spelling, grammar, and punctuation

Professional copywriters go to great lengths to create emails with well-tested content, subject line, call-to-action etc. It is very likely that any email that contains poor grammar, punctuation or shows an illogical flow of content is likely written by inexperienced scammers and are fraudulent.

2. Asking for personal information

Established brands never ask you sensitive information via email. Any messages asking to enter or verify personal details or bank/credit card information should be treated as big red flags.

3. Alarming content full of warnings and potential consequences

Hackers can send messages that cause alarm by telling you things like one of your accounts has been hacked, your account is expiring, and that you may lose some critical benefits immediately, or some other extreme condition that puts you in panic. Such content is typically formatted to create alarm and a sense of urgency with the intent of driving the user to take immediate action.

Red Flags That Will Help You Spot **Phishing Scams & Attacks:**

4. Urgent deadlines

In this pattern, hackers send out an email about some pending deadline. For example, a hacker could send out a renewal email about an expiring insurance policy, or a limited validity discount on some deal that might be of interest to the target. Typically, such emails lead the users to data harvesting sites that end up stealing valuable personal or financial information.

5. Offer of large financial rewards

This pattern includes emails claiming that you have won a lottery when you never purchase one, offer of a large cash discount on something that you never purchased, large prize money in a contest that you never enrolled for and so on. The actual intention is usually to direct you to a site where the scammers can get your personal or financial information.

THINK BEFORE YOU CLICK!

It's fine to click on links when **you're on trusted sites.**

Do not click on links that appear in random emails or instant messages. Be cyber-smart.

Hover over links that you are unsure of before clicking on them. Do they lead where they are supposed to lead?

A phishing email may claim to be from a legitimate company and when you click the link to the website, it may look exactly like the real website. **The email or website may ask you to fill in personal information when the email itself did not contain your name.**

Most phishing emails will start with **"Dear Customer"** so you should be alert when you come across these emails.

When in doubt, **go directly to the source by picking up the phone** to double check rather than clicking a potentially dangerous link.