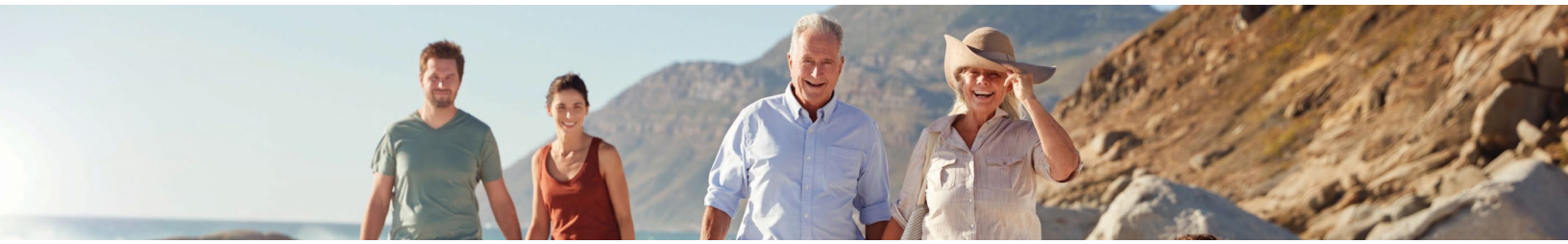
CIBC

CIBC PRIVATE WEALTH



PRESERVING FAMILY WEALTH

Protecting what you have built: Household, liability, and online risk

Safeguarding family wealth requires recognizing, acknowledging and preventing exposure to risks—and risks come in all shapes and forms, including people, computers or legal actions. All have the potential to damage your financial security and your family's wealth. And, in large part, all are based on issues of trust. Three such risks are the following:

1. Household management[1]

When a family requires staff—whether a housekeeper, a nanny, an elder caregiver or any other household role—the family becomes an employer and must carry out all the roles of an employer. This may include finding candidates, managing payroll, and providing a safe work environment. Steps you may take as an employer to avoid the loss of time and money from employee turnover or a potential lawsuit include the following:

- Remember that your home is the employee's workplace and you have a professional relationship with each other
- Prepare a good job description for each role
- Understand employment law and tax reporting requirements
- Screen potential employees with a background check and personality and skill tests
- Consider engaging a professional staff hiring and management service
- Obtain an employment practices liability insurance (EPLI) policy

2. Liability exposure through lawsuits[2]

Lawsuits can have disastrous financial results if you aren't prepared for the possibility of being sued. Many families often underestimate the cost of potential damages in a lawsuit and don't realize the affordability of the insurance that may help cover such damages. Some of those potential lawsuits and their related insurance protections include:

- Liability from an accident causing harm or death could be covered with an adequate umbrella policy
- Liability related to household staff—including wage and hour claims, discrimination and other claims–could be covered with an EPLI policy
- Liability related to serving on a board of directors or owning a private company with a board of directors could be covered with a directors and officers (D&O) policy

3. Online risk[3]

An increasingly digital world presents new challenges on a regular basis. Smartphones are ubiquitous, and many people rely on them for a wide spectrum of day-to-day activities, from banking to shopping to photo storage. When "everything online" is the norm, it is important to consider how much others may know about us. Steps to take to minimize your online exposure include:

- Consider how important privacy is to you
- Minimize your online footprint
- Understand your devices and software, mitigation tools and what information can be collected about you
- Consider cyber insurance, which may be included in your homeowner's liability policy

For more information on household, liability and online risks, visit our *Preserving Family Wealth* resource page.

[1]Teresa Leigh, founder and CEO of Teresa Leigh Home and Family Office, contributed to this content.
[2]John Pullara, Vice President and team leader at EPIC Insurance Brokers, contributed to this content.
[3]Craig Sherwood, partner at Shambliss Security in Schaumburg, Illinois, contributed to this content.

Phishing, vishing and smishing

Online criminals represent a persistent and evolving threat to our information security. Exploiting our willingness to share information and connect with others online, cybercriminals target individuals and organizations to gain access to sensitive information. They do this by phishing. Cybercriminals create and send emails that trick the recipient into divulging personal information, performing an action that is fraudulent, or downloading malware by opening attachments or clicking on links. The emails often look real and look like they come from legitimate companies. Even the most alert and aware can be fooled.

Recognizing common phishing tactics

Cybercriminals hook you by taking advantage of habits and emotions that drive action, such as fear, urgency, curiosity, compassion and greed, to entice you to click on a link or open an attachment.

- **Greed:** Messages may promise financial rewards (e.g., “Click here for a gift card”).
- **Fear:** Cybercriminals try to create heightened anxiety (e.g., “The following charges have been applied to your credit card. Click here to view invoice details”).
- **Curiosity and desire:** Messages may offer additional information related to matters of personal interest (e.g., celebrity news, hobbies, current events, social and sporting events).
- **Compassion:** Cybercriminals use the generosity and caring nature of recipients (e.g., “Click here to donate to a charitable organization”). Spear phishing is a very targeted form of phishing that uses emails that appear to come from a known source (e.g., your manager, a vendor, a client, your friend). Since they appear to be normal, relevant, and/or from a trusted source, they can be particularly difficult to spot.

Cybercriminals are not just using email to trick victims. They are also:

- **Vishing:** using the telephone
- **SMishing:** using text (SMS) messaging

1. What to do with a suspicious email or text. Before responding, ask yourself:

- Do I know the sender?
- Am I expecting this message?
- Is the message out of character, inconsistent or poorly written?
- Is this how the sender typically communicates with me?
- Is the message provocative and compelling me to click on embedded links or attachments?

2. Still suspicious?

- Do not click on any embedded links or file attachments.
- Hover over any links—without clicking—to investigate where the link will go. Does the main part of the link match what you would expect from the sender?
- Do not reply to the message sender, even to ask the sender to stop contacting you. Test the authenticity of the message using trusted alternative contact information not provided in the email/text.
- Do not copy anyone on these messages as this increases the chances that the email/text could be opened
- and the malware released.

In the past, grammar and spelling mistakes, formatting errors and generic salutations (e.g., “Dear Customer,”) were common phishing red flags. While these can still be warning signs, the increased sophistication of cybercriminals means they are not as reliable indicators as they once were.

What to do with a suspicious phone call (vishing)

- Ask for the caller’s name, phone number and department (or organization if it is someone claiming to be from a supplier). Tell the caller that you’ll get back to them.
- Before providing any information, attempt to verify the caller’s information using an alternate trusted source, such as contact information from a website.
- Do not be pressured into providing information or taking some action. Threats are common tactics.
- If you’re uncomfortable with the questions being asked over the telephone, do not respond. Tell the caller you are ending the conversation and then call back using an independently verified phone number.
- If you receive a phone call or voicemail message you suspect might be “vishing” and feel you must respond, contact the organization using trusted alternative contact information not provided in the message.