LaFleur & Godfrey
PRIVATE WEALTH MANAGEMENT

625 Kenmoor Avenue SE, Suite 209
Grand Rapids, MI 49546

The Investment Letter

Volume 97 No. 1

February 2026

Protect Yourself from Cybercrime

We often receive calls from clients targeted by bad actors – attempts to hack email accounts, fraudulent "tech support" calls, and messages forged to appear as if they have come from a trusted institution.

The cybercriminals perpetrating these crimes are persistent, well-funded, and constantly refining their tactics, with increasingly sophisticated schemes that dupe even the savviest among us. Becoming the target of a cybercrime is even less today a reflection of poor judgment or inexperience.

As more of our personal and financial lives have moved online, criminals have followed. Today's methods are designed to deceive people who are otherwise careful, informed, and very much "in the know."

So, how do you best protect yourself and your loved ones? The good news is that protecting yourself does not require technical expertise, an advanced degree in finance, or certifying your knowledge of cybersecurity. You need awareness, patience, and a willingness to hit "pause" when things do not sound right.

How to Protect Yourself from Cybercrime

1.Slow Down. Trust Reason Over Reaction

Scammers rely on urgency. Criminals know that pressure pushes victims to act before they have time to think, verify, and sense the unfolding of a scheme.
You may be told that:

- You must make a wire transfer immediately
- Your account will be frozen unless you act now
- You need to address an urgent technical problem
- You have been offered a financial opportunity, but only for a "limited time"

Legitimate financial institutions won't pressure clients to move money quickly via unsolicited emails, pop-up messages, or phone calls. Government agencies don't demand payment through wire transfers, gift cards, or cryptocurrency. If the details of an investment opportunity start to fall apart under careful review, it's time to hit pause.

When you receive a request involving money, take a moment. Walk away from the computer or phone. Take time to think and consider talking about the details with someone you trust. Those extra few moments can thwart many scams. Acting quickly may feel decisive and empowering, but this is exactly what scammers rely on.

2.Treat Digital Communications with Healthy Skepticism

Email, text messages, and online pop-ups are now the most common entry points for cybercrime. When sending these messages, scammers often impersonate banks, technology companies, family members, or friends you trust. They can spoof caller ID notifications, email addresses, and website URLs so they appear convincingly authentic. Look for these warning signs:

- Does the message feel slightly "off" or out of character?
- Do attachments or links seem out of place or unnecessary?
- Is the communication requesting your password, a code, or other account information?
- Does the message contain poor grammar, misspellings, or unusual urgency?

Avoid following the links embedded in these emails or texts. If in doubt, contact the company or institution through the contact information on their website. Verify the authenticity of the message. Don't trust the contact information provided in the message itself.

3. Think of Your Passwords as Digital Front Doors

Your online accounts deserve the same degree of security as your physical home. Change your passwords regularly and avoid weak, easily guessed passwords. Update outdated software on your phone and computer to make it harder for criminals to gain access to your devices.
When strengthening your digital front door, a few simple practices go a long way:

- Choose strong, unique passwords for your online accounts
- Avoid reusing the same passwords across multiple websites

- Enable two-factor authentication when available
- Update your operating system, browser, and antivirus software as prompted.

Take care when you share information publicly. Details about birthdays, pet names, the schools you've attended, and family relationships can be harvested and used to guess passwords or answer your security questions. Quizzes on social media may appear harmless, but criminals can use this information to hack into your accounts.

4. When a Message Asks You to Move Money, Be Especially Skeptical

Requests to transfer funds deserve extra scrutiny, particularly when they ask you to execute a wire transfer. Wires move quickly and it's difficult, if not impossible, to reverse a wire after it's been sent.

These kinds of scams frequently involve:

- Fraudulent invoices
- Sudden changes to payment details, such as being asked to send funds to a different account
- Emails impersonating business contacts requesting payment.

Always verify wire instructions verbally using a phone number you already trust. Vet requests to change payment information before sending funds. Never rely solely on the information in one email, even if the message appears to be legitimate. Scammers can compromise or spoof an email account without the owner realizing it.

For an added layer of protection, you may ask LaFleur & Godfrey to require verbal confirmation before executing account instructions, especially those involving withdrawals or transfer requests. This may feel inconvenient, at times, but this extra precaution can prevent irreversible mistakes.

5. Name a Trusted Contact

You can choose a trusted contact person, e.g., a spouse, adult child, sibling, or close friend, who can be contacted when questions arise about unusual activity, suspicious requests, or potential financial exploitation. Trusted contacts can't transact on your account, but they serve as a second set of eyes when something seems "off."

Scammers rely on isolating their victims. They urge secrecy and discourage you from seeking outside consultation. Trusted contacts help thwart that strategy and can help you see through the urgency and confusion scammers try to create. We can help clients:

- Designate a trusted contact for their accounts
- Inform that person that they have been named and why.

In moments of stress, illness, or uncertainty, having someone who can help confirm a financial decision can be invaluable.

Pause. Ask Questions.

Cybercriminals prey on cultivating trust that they create in the heat of an urgent moment when you haven't had time to carefully consider what they're asking. To best arm yourself against their schemes, become deliberate in vetting the messages you receive online, over the phone, and through the mail. The goal isn't to become fearful or suspicious of every message, but to exercise care.

Be willing to ask questions. Trust your intuition when something feels wrong. If you are ever unsure, we encourage you to reach out to us, your trusted contact, or the company or institution itself through independently verified contact information. We would much rather answer a question today, than face an unfortunate problem tomorrow.

Inside the Office

We're planning a client webinar aimed at reviewing this information – please watch for an upcoming invitation. The goal will be to provide tips and insights on how to protect yourself, along with your family members. Children and elderly parents are often the victims of cyberattacks! The webinar will be purposefully designed for all digital experience levels with practical solutions anyone can use.