



OPTIMUM EXPERIENCE

NEWSLETTER FOR CANANDAIGUA NATIONAL BANK & TRUST OPTIMUM CHECKING CUSTOMERS

How to Protect Yourself from Cyber Threats

In today's world — where data breaches are common occurrences — it's especially important for you to understand the digital risks you face. Are you doing all you can to mitigate the risk of a cyberattack? According to Lexis Nexis, 4,500 data breaches have occurred in the last 15 years, with 45% of Americans suffering some form of personal information compromise in the last 5 years.

What are your vulnerabilities?

How are your systems protected? Do you collect and store personal information, such as credit-card information, Social Security numbers, and birth dates? If so, how is this information stored and who may access it? Do you store it in multiple locations and formats? Are these files password protected and, if so, are you using multiple complex passwords? Do you have Wi-Fi accessible to others?

Tips for security

When monitoring your security, ensure you have firewall and encryption technology that protects your Internet connections and Wi-Fi networks. Make sure your computers have antivirus and anti-spyware software installed and updated automatically. Use complex passwords that are changed regularly, and do not share your passwords with anyone. Keep only personal data that you actually need and dispose of it securely as soon as it no longer serves a purpose. Back up critical information and data on a regular basis and store the backups securely. Utilize two-factor authentication within apps wherever offered. If you've suffered a cyber fraud event, consult an IT professional to check your systems as soon as possible.

Redundancy is key

In writing or speaking, redundancy is typically not recommended unless you're really trying to drive a point home. When it comes to your digital life, however, redundancy is not only recommended, it's critical. That's because redundancy means having multiple data backups stored in different locations. Here are some ideas for redundancy when backing up your data:

- If you have digital assets that you don't want to risk losing forever—including photos, videos, original recordings, financial documents, and other materials — you'll want to back them up regularly, in at least two locations, preferably in multiple file formats. And it's not just materials on your personal computer, but your mobile devices as well. Depending on how much you use your devices, you may want to back them up as frequently as every few days.
- Ensure that at least one backup copy is stored offsite. You could store your external hard drive in a safe-deposit box or at a trusted friend or family member's house. Cloud storage is also considered offsite.

More about cloud storage

Cloud storage — using Internet-based service providers to store digital assets such as books, music, videos, photos, and even important documents including financial statements and contracts — has become increasingly popular in recent years. But is it right for you? If a cloud service is one of your backup tactics, be sure to carefully review the company's policies and procedures for security and backup of its servers. Another good idea is to encrypt (that is, convert to code) to protect sensitive documents and your external drives. Other considerations include:

- Evaluate the provider's reputation. Is the service well known, well tested, and well-reviewed by information security specialists?
- Consider the provider's own security and redundancy procedures. Look for such features as two-factor authentication and complex password requirements. Does it have copies of your data on servers at multiple geographic locations, so that a disaster in one area won't result in an irretrievable loss of data?
- Review the provider's service agreement and terms and conditions. Make sure you understand how your data will be protected and what recourse you have in the event of a breach or loss. Also understand what happens when you delete a file —will it be completely removed?
- Consider encryption processes, which prevent access to your data without your personal password (including access by people who work for the service provider). Will you be using a browser or app that provides for data encryption during transfer? And once your data is stored on the cloud servers, will it continue to be encrypted?

Be aware

Ensure that you understand the risks associated with phishing emails, as well as "social engineering" — manipulative tactics criminals use to trick employees into divulging confidential information. Remember, most companies generally do not contact you asking for any user-specific information such as username, password, or other personal information.

The FBI regularly publishes articles on trending fraud schemes and allows victims to report schemes via their Internet Crime Complaint Center (IC3). For more information, visit www.fbi.gov/scams-and-safety.

*Todd Billcliff is an Assistant Vice President,
Fraud Risk Officer and CFE.
He can be reached at (585) 419-0670
x50641 or TBillcliff@CNBank.com*



A Financial Wellness Plan Can Help Pave the Road to Retirement

If we've learned any lesson over the past year, it's that no matter how carefully we plan and prepare, we'll likely encounter unexpected hurdles. While a global pandemic has certainly underscored the need to pay close attention to our physical wellness, it has also revealed the need to shore up our financial wellness.

According to PwC's 9th Annual Financial Wellness Survey conducted in January 2020, financial matters were the top cause of stress for employees even well before the pandemic hit in earnest. More than one-third of full-time employed millennials, Gen Xers, and baby boomers had less than \$1,000 in emergency savings. Only 29% of women said they would be able to cover their basic necessities if they found themselves out of work for an extended period, compared with 55% of men. And more than half of millennials and Gen Xers and 35% of baby boomers said they would likely use their retirement funds for something other than retirement, with most noting it would be for an unexpected expense or medical bills.¹

Although tapping your retirement savings can help you get through a crisis, it can hinder your ability to afford a comfortable retirement. Having a plan to guard your financial wellness throughout your working years can help you avoid putting your retirement at risk.

What Is Financial Wellness?

The Consumer Financial Protection Bureau (CFPB) defines financial well-being as:²

- 1) Having control over day-to-day and month-to-month finances. In order to achieve this, your expenses need to be lower than your income.
- 2) Maintaining the capacity to absorb a financial shock. This typically refers to having adequate emergency savings and insurance.
- 3) Being on track to meet financial goals, meaning you have either a formal or informal plan to meet your goals and you are actively pursuing them.

- 4) Having the financial freedom to make choices that allow you to enjoy life, such as a splurge vacation.

The CFPB has identified several key factors that contribute to an individual's ability to achieve financial well-being. Among them are: (1) having the skills needed to find, process, and use relevant financial information when it's needed; and (2) exhibiting day-to-day financial behaviors and saving habits.

Assistance Is Available

Many employers have begun offering financial wellness benefits over the past decade. These programs have evolved from a focus on basic retirement readiness to those addressing broader financial challenges such as health-care costs, general finance and budgeting, and credit/debt management.³

If you have access to work-based financial wellness benefits, be sure to take time and explore all that is offered. The education and services can provide valuable information and help you build the skills to make sound decisions in challenging circumstances.

In addition, a financial professional can become a trusted coach throughout your life. A qualified financial professional can provide an objective third-party view during tough times, while helping you anticipate and manage challenges and risks and, most important, stay on course toward a comfortable retirement.

CNB Can Help

If you have questions about your financial goals, please contact me or your local Bank Office representative to schedule an appointment.

Amy Flaitz is an Assistant Vice President, Manager of the Victor Community Office. She can be reached at (585) 742-4950 x40220 or AFlaitz@CNBank.com



©2021 Broadridge Investor Communication Solutions, Inc. All rights reserved. 1) PwC, May 2020 2) Consumer Financial Protection Bureau, January 2015 3) Employee Benefit Research Institute, October 2020

Member FDIC



Annual Picnic Postponed to 2022

While restrictions have recently relaxed and we are gradually returning to in person events, we will not be hosting our Annual Picnic in August 2021. However, we look forward to safely celebrating this event with you once again in 2022.



CNB Podcasts

Introducing the CNB Financial Wellness Show Podcast

Hear from Canandaigua National Bank & Trust's financial professionals as they discuss strategies for improving your financial wellness.

Subscribe to our podcast on Apple Podcasts* or Google Podcasts or listen online at CNBank.com/CNB_Podcasts.



*Apple, the Apple logo, and Apple Podcast are trademarks of Apple Inc., registered in the U.S. and other countries. App Store is a service mark of Apple Inc., registered in the U.S. and other countries.

CNC Shareholder Corner



Canandaigua National Corporation

Up-to-Date Stock Information & More

For more information on up-to-date CNC Stock pricing, CNC Annual Report, Statement of Condition, and more, visit our Shareholder web page.

CNBank.com/ShareholderRelations