Summer 2017

Cambridge Quarterly NEWSLETTER

A personal finance newsletter presented by Cambridge Credit Counseling

WHAT'S INSIDE?

67 Hunt Street • Agawam, MA 01001 • (800) 527-7595 • www.cambridge-credit.org

GOING ON VACATION?

MAKE SURE YOU TEST YOUR AC BEFORE THE HOTTEST TEMPERATURES ARRIVE. FIRST, CHECK TO MAKE SURE THAT THE FILTER IS CLEAN. NEXT, CHECK TO SEE IF YOUR THERMOSTAT NEEDS NEW BATTERIES; YOU SHOULD SEE A BLINKING LIGHT, OR A BATTERY GAUGE INDICATING THAT YOUR BATTERY MIGHT BE LOW. THOSE ARE THE EASIEST WAYS TO REJUVENATE YOUR AC UNIT.

DATA SECURITY IN TROUBLED TIMES

Last summer, we talked about how to keep your identity safe while making purchases with your debit card at big-name retailers. Now, we're hot on the heels of the ransomware virus, WannaCry, which swept the globe when it attacked over 150 countries, 10,000 organizations, and 300,000 individual computers after a hacker exploited a security flaw found in all Windows operating systems. It locked down users' computers and requested that victims pay a fee of $300 to recover their information. The longer the user waited to make the payment, the more the price would increase and data would be destroyed. The virus was so sophisticated that it was able to cause 16 hospitals in the UK alone to shut down, putting lives at risk.

The threat of infection from a digital virus is becoming very real, especially with all of the personal information that we store on our devices (whether we know it or not). We'd like to talk to you about what you can do to protect your personal data from such viruses. Please, keep in mind that these are only a few precautions you can take, and we're discussing them briefly. If you suspect you have an infected device, consult a professional as soon as possible.

Here's how to protect yourself:

1.) Install and enable automatic updates to your software if they're not already set up. Security updates happen often and can be installed while you're doing other things on your computer. You probably won't even notice, and your operating system's security will be up to date, even on older systems. Make sure you check that your operating system has no pending updates. After WannaCry, Windows sent out a huge security patch to prevent uninfected computers from contracting the virus. Users who did not have the updates set up to automatically run missed out on Window's speedy response.

SONIA HAS BEEN WITH US FOR FOUR YEARS AND SHE IS MUCH MORE THAN OUR RECEPTIONIST, SHE'S THE FIRST FACE OUR CLIENTS SEE WHEN THEY VISIT OUR OFFICE. WE DEPEND ON HER FOR HER WARM SMILE AND SUNNY DISPOSITION!

"THERE IS NOT A MORE REWARDING FEELING THAN BEING ABLE TO MEET AND WORK WITH SO MANY GREAT PEOPLE AND KNOW THAT THEY APPRECIATE WHAT YOU DO. I CAN TRULY SAY THAT I AM A VERY HAPPY AND PROUD MEMBER OF OUR CAMBRIDGE GROUP AND ENJOY WORKING WITH ALL OF MY FELLOW EMPLOYEES TO ENSURE THAT WE PROVIDE THE BEST CUSTOMER SERVICE EXPERIENCE TO ALL OF OUR EXISTING AND POTENTIAL CLIENTS."

EMPTY OUT YOUR FREEZER AND MAKE AN INVENTORY OF WHAT YOU HAVE. WHILE IT'S EMPTY, CHIP OFF THE ICE THAT MIGHT HAVE BUILT UP DURING THE WINTER. REGULARLY CLEANING OUT YOUR FREEZER ENSURES THAT YOU'RE NOT LETTING ANY FOOD GO TO WASTE.

PROTECT YOUR HOME AGAINST BUGS. CHECK THE CAULKING AROUND YOUR WINDOWS AND DOORS TO START. IF YOUR HOME IS PRONE TO A CERTAIN KIND OF INSECT, YOU CAN PREPARE ACCORDINGLY. FOR INSTANCE, HOMES THAT HAVE ANTS USUALLY SEE THEM EVERY YEAR. PREPARE BY LAYING OUT ANT TRAPS IN KEY AREAS BEFORE THE PESTS HAVE A CHANCE TO RE-ESTABLISH THEMSELVES.

2.) Back up your data. Everyone has heard this, but very rarely do people put it into practice. Users who were affected by WannaCry would have felt confident that their files were safe if they had a backup of their information stored on an external hard drive or a cloud. Consider backing up your data monthly or even weekly so that you have a current copy of your system and all of the data on it in case of emergency.

continued on back

FREE ANTI-VIRUS SOFTWARE IS OUT THERE

We looked into the top rated, free antivirus software available for 2017 and found that each of the most popular choices has its pros and cons.

Microsoft Security Essentials – Free for Windows users with Windows Vista/7. It provides anti-spyware, antivirus, scanning and cleaning, and all around 'comprehensive malware protection.' Users with Windows 8 and higher have Windows Defender already included.

Avast Free Antivirus – Available for Windows, Mac, and Android. Avast was the most popular free antivirus product on the market in 2015. Avast provides computer security, browser security, antivirus software, anti-phishing, anti-spyware, and live updates to ensure that your Avast software is always up to date. Avast has another version with more features for $80 a year.

Avira Free Antivirus 2017 – Available for Windows 7 and up. Avira includes an antivirus, password manager, and System SpeedUp, which is designed to help your machine run faster by freeing up disk space with your permission (this can also help your battery life last longer). This software is highly effective and customizable, although older computers may experience slower performance during active scans. Avira does have a pay version with more features for $100 a year.

Bitdefender Antivirus Free Edition – Available for Windows, Mac, and Android. The free version of this software offers the same antivirus protection as its commercial counterpart. It also offers great anti-phishing protection. In short, Bitdefender is very good at what it does, protecting against malware. Bitdefender does have a pay version with more features for $50 a year.

PRODUCE IN SEASON FOR SUMMER

1.) CUCUMBERS
2.) WATERMELON
3.) TOMATOES
4.) CANTALOUPE
5.) CORN
6.) BLUEBERRIES
7.) SUMMER SQUASH
8.) PEACHES
9.) GREEN BEANS
10.) KIWI

2.) Turn off your devices when you're not at home. If you device is 'asleep' while you are away it is still connected to the internet, and it could be in danger of an attack.

4.) Your password has to change regularly. Many people use the names of their pets, their vehicle make or model, or simply the word 'password'. A hacker wouldn't have to look any further than your social media pages. If those don't work, the top six passwords of all time include "password," "123456," "12345678," "1234," "qwerty," and "12345." Do you see a pattern here? The overwhelming majority of people have a password that is either very common or very easy to deduce. Even worse, most of us use the same or very similar passwords for all of our log-ins. If that's the case, once one of your passwords has been found out, it's going to be easy for a hacker to gain access to another one of your accounts. Change your password in creative ways. Try making shapes out of characters on the keyboard or using a combination of vocabulary words to make a passphrase. Don't be afraid to write down your passwords and keep them hidden, but near your computer if you need to reference them.

5.) Answer your emails with extreme prejudice; one in four email accounts is hacked. The easiest way to infiltrate your system is through email. Malicious emails are not as easy to spot as you might believe. Many hackers will pose as people you know, perhaps with the subject line of "Hey! I haven't seen you in so long," or, "Check out this throwback picture of us." These emails will ask you to click a link or download an attachment which will contain the virus. Once you click on one of these, your computer will be infected. Remember, you might not think that you have anything important in your email, but you do! Your email is interconnected with all of your other accounts (any account that asks for it, like social networks, credit cards and online shops), password resets, pin numbers, tax forms, and other valuable personal information that a hacker could use to gain access to your other online accounts.

Data security does not happen on its own. It's up to you as a responsible user to make sure that you are taking every precaution necessary to keep your information safe. Nevertheless, don't be afraid to explore using technology to make things easier for you. Too often, people are so afraid of compromising their data that they won't take advantage of some of the benefits that technology has to offer. For instance, paying bills online is one of the fastest ways to pay, and oftentimes comes with benefits for auto-enrolling in automatic payments. If you are using features like these on your password-protected Wi-Fi at home, as long as you use a strong password, you should be fine. Also, purchasing products online can save you money. There are precautions you can take if you're feeling uneasy about shopping on the Web. After you enter your card information during check-out, most online retailers will ask you if you would like to save your card information to make future purchases faster. Do not do this. If the online retailer is hacked, your card information will not be available to them. Stay safe!