August 2019

Microsoft REGISTERED Refurbisher

The next General Meeting of CCCGC will be **August 6, 2019**

Charlotte Bytes

Editor A Yvette Pilch
Asst. Editor Rose Kopenec

See us on the Web
www.cccgc.info

Official Publication of the Charlotte County Computer Group Corp.

PROMOTING COMPUTER LITERACY AND EDUCATION IN CHARLOTTE COUNTY

The largest gathering of computer knowledge in Charlotte County

VOL. XXXI

No. VIII

Inside this issue:

Charlotte County Computer Group Corporation

2280 Aaron Street
Port Charlotte, FL 33952
Phone: 941-585-0356
941-625-4175 x244

E-mail: cccgcoffice@gmail.com

CCCGC

The President's Platform

Dear Members,

Linda Corrick is our Volunteer of the Month.

Reminder:

Lydia is still in need of help in the repair department. If you are interested in helping in this area, please contact me or Lydia.

If you have any suggestions of topics for the meeting presentation or if you would like to present a topic, please let me know. I hope everyone enjoys the meetings.

If I have not personally met some of you, please stop in the office or come up to me at our regular meetings. I would greatly enjoy getting acquainted with you.

The last quarter of 2019 is getting closer (can you believe it!!). Nominations of officers and directors will be starting soon. The positions of Vice-President, Secretary, and Director are open. The slate of Board members will be nominated in November and voted on in December. Those of you that are interested in a position please speak with Yvette.

We need volunteers for the Board!

I hope to see you all at our next meeting on Tuesday, August 6.

Grover

Guidelines for Attending Classes

Please be sure to notify the instructors or Office when planning to attend class by either email or the online entry signup form.

WELCOME

New Members

Mimi Barone		
Mary Benz		
Larry Benz		

The Executive Board and Members of CCCGC welcome each of you to the group. We're here to help. Membership has its privileges.

If you have any questions, concerns or need computer help, please contact us at the office. We will endeavor to help you any way we can.

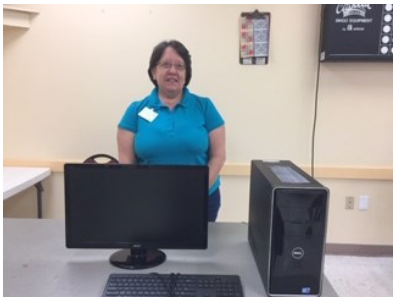
July Program Highlights

Volunteer for the Month of July

Joanne Pisaturo

FREE Membership Winner
Larry Spieldenner

Computer Raffle Winner
Joyce Lyons



50/50 Raffle Winner

George Kopenec

FREE Raffle Winners

Richard Bader
Charlie Burns
Ruth Wagley
Glenn Taylor
Alfonso Falasco

CCCGC

Microsoft® REGISTERED Refurbisher

For more information go to
www.cccgc.info

View/download Bytes

Please be sure to register online for classes

Next Meeting is August 6, 2019

For the latest Classes & Events Calendar

Please click on button below

Events Calendar

The Charlotte County Computer Group Corp.

Is a non-profit 501(c)3 organization as classified by the Internal Revenue Service.

Donations, gifts, bequests, legacies, devices and transfers are deductible under federal laws.

PROMOTING COMPUTER LITERACY AND EDUCATION IN CHARLOTTE COUNTY

TechRegar just tech stuff

We're on the Web
www.cccgc.info

Articles in the Bytes are courtesy of the following Tech Sites

Digital Citizen

www.dickevanstraining.blogspot.com

makeuseof

dotTech

Windows Secrets
Everything Microsoft forgot to mention.

Into Windows

daves.computer.tips

the How-To Geek
Computer Help from your Friendly How-To Geek

ghacks.net

Official Publication of the
Charlotte County Computer Group Corporation
2280 Aaron Street, Port Charlotte, FL 33952

Information: (941) 585-0356 or (941) 625-4175 x244 www.cccgc.info or www.cccgc.net

July 2 , 2019 Meeting Pictures

Official Publication of the
Charlotte County Computer Group Corporation
2280 Aaron Street, Port Charlotte, FL 33952

Information: (941) 585-0356 or (941) 625-4175 x244 www.cccgc.info or www.cccgc.net

Notes from July 2, 2019 Meeting

Start Screen Or Start Menu
By Dick Evans

I never gave it much thought but there is a difference between start screen or start menu. On Windows 8 we were given a Start Screen. To get to the desktop we had to take another step. Navigating the Start Screen was a challenge for us users that came up the path of Windows versions. It was a new concept and I for one did not care for it.

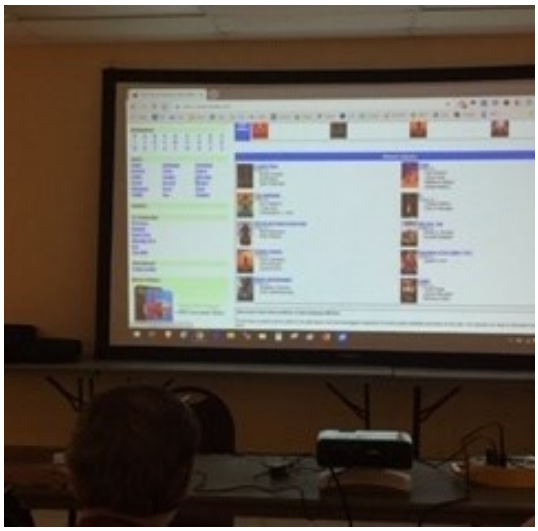
If you have a touch screen it is much easier to use the start screen as all you have to do is touch the Icon to start any of your applications. With a mouse just point and click once.
The Start Menu

With Windows 10 we can have either the start menu or the start screen as default. Out of the box we get the start menu. It looks much like Windows 7 with a taskbar and a desktop with icons. It only took a few times using it to feel comfortable with it.

However the Windows 8 start screen made It so much easier to use. Especially with a touch screen. All you had to do was look at the screen and tap the icon you wanted to activate.
This makes it much easier for non computer people to take advantage of the internet

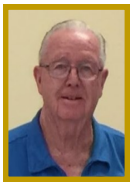
Tablet Mode
All additional and more info is on our website

www.cccgc.info.



Officers and Board of Directors for 2019

OFFICERS



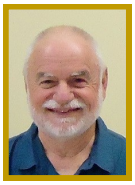
President:
Grover Mudd

Vice President:
Yvette Pilch

Secretary
Lydia Rist

Treasurer
Harold Nixon

DIRECTORS



Dick Evans

George Kopenec

Ron Muschong

Joanne Pisaturo

Donna Whalen

August Volunteer of the Month:

Linda Corrick has been a Wednesday volunteer on the desk for many years.

She also inputs info which (includes members payments and all monies donated to the Club) into our database.

Linda also has served as nominating Chairperson and December vote-counter. She performs the swearing-in of newly elected officers.

Linda helps at the tables on meeting nights, and she is a hard worker with a great sense of humor.

the How-To Geek Computer Tidbits

Computer Help from your Friendly How-To Geek

How Criminals Order Phones in Your Name (and How to Stop Them)

Josh Hendrickson@canterrain

July 12, 2019

A new type of phone theft is on the rise. Instead of stealing phones directly from you, thieves impersonate you to get brand new smartphones from your cellular carrier and stick you with the bill. Here's what's going on.

What Is Account Hijacking?

Outright smartphone theft is getting harder to pull off and less lucrative. We're more careful with our phones than we used to be and—starting with the iPhone—more smartphones offer encryption and lost phone tools out of the box. So, some criminals have adopted a new tactic. Instead of messing with stolen phones and worrying about activation problems, they pose as you and order new phones on your account.

The scam works well for a variety of reasons. The criminal gets to take advantage of any phone deals your account is eligible for, paying as little as possible up-front (perhaps, even nothing at all), and you may not notice until it's too late. Upgrading your existing lines is the more noticeable method because your phones stop working, so some criminals add new lines, instead. With that route, you may not realize what's happened until the next bill comes. And, if you have your phone bill set up for automatic payment, you could miss it for longer than that.

In some cases, the point isn't to steal phones. Criminals may upgrade your lines as a means to take your number through SIM swapping. Your phone number is transferred to a phone they have, which they can then use to hijack any accounts that rely on your phone number as a recovery option.

How Criminals Hijack Cell Phone Accounts

At this point, you might wonder how a criminal can buy smartphones with someone else's account. Unfortunately, we've discovered more than one answer to that question.

Sometimes, the perpetrator steals your identity, creates a fake ID with your name and his photo, and then goes to a retail store to buy the phones. You might think that method could only occur close to where you are but, as Lorrie Cranor, a former chief technologist for the FTC found out, that's not the case at all. She discovered her phones turned off after someone posing as her, multiple states away, upgraded her lines to new iPhones. You can find similar complaints on phone carriers' forums as well.

In 2017, Cleveland police arrested three men after linking them to $65,000 worth of cell phone theft, mostly through the use of fake IDs.

the How-To Geek
Computer Help from your Friendly How-To Geek

Computer Tidbits cont.

In other cases, simple phishing tactics are at play. In early 2019, Verizon customers in Florida started receiving calls about suspected fraud. The representative told the victims they needed to verify their identity and, to do so, Verizon would send a PIN. They would then need to read the PIN to the person on the phone.

But the person on the phone wasn't an employee from Verizon. It was the fraudster the victim had just been warned about. In this case, the thief generated an actual Verizon PIN, most likely by using the account recovery process. When the victim received the PIN and handed it over, they gave the criminal the very details they needed to get into the account and order new smartphones. Thankfully, Verizon employees noticed other red flags and called the police, but that doesn't always happen.

In late 2018, twelve people were accused of hacking into people's online accounts, adding or upgrading lines, and then shipping the new hardware elsewhere. Before police caught up with them, it's believed the perpetrators managed to obtain over $1 million worth of devices. They used information purchased on the dark web from data breaches or, in some cases, sent phishing messages to steal account info.

What to Do if Your Account Is Hijacked

1. **Call the companies where know fraud occurred.**
2. **Place a fraud alert and get your credit reports.**
3. **Report identity theft to the FTC.**
4. **You may choose to file a report with your local police department.**

If you're the victim of account hijacking, it may feel like there's nothing you can do, but that's not true. You shouldn't have to pay for a service you didn't want, and phones you don't have. Get a pen and paper and take notes on the process. Write down which companies you called, the date and time, and the name of any person you spoke with. Take notes on what the company representatives say—especially if they promise to take action or ask you to follow up with more information or paperwork. The FTC put together a helpful checklist to follow, and we'll be covering some of those steps as well.

First, call your phone carrier and explain the situation. Ask if they have a fraud department. If they do, ask to be transferred. Explain the situation and ask for help solving the problem. Find out precisely what proof they need from you and write everything down. You should also ask if your account can be frozen and if you can add a PIN validation (or other security measures) to prevent anyone from adding more lines to your account.

First, call your phone carrier and explain the situation. Ask if they have a fraud department. If they do, ask to be transferred. Explain the situation and ask for help solving the problem. Find out precisely what proof they need from you and write everything down. You should also ask if your account can be frozen and if you can add a PIN validation (or other security measures) to prevent anyone from adding more lines to your account.

Next, place a fraud alert on all your credit accounts. You might also consider freezing your credit. A credit freeze should prevent anyone from opening an entirely new account in your name but, unfortunately, it might not prevent upgrade and add-a-line fraud. Many phone carriers bypass a credit check in favor of checking billing history for existing customers. Still, a credit freeze could prevent other kinds of fraud, so it's worth it.

the How-To Geek
Computer Help from your Friendly How-To Geek

Computer Tidbits cont.

With a credit freeze in place, it's time to report the fraud to your local police department. Call or visit them and ask how to report the situation. Be sure to have any proof on hand, like bills from the added lines. Explain what happened and get a copy of all the paperwork.

Now, contact your phone carrier again with any paperwork they requested (including the police report) and ask how to reverse all charges if it hasn't already been done.

Be prepared for this process to take some time—sometimes, days or weeks. Keep a log of everyone you contact and every step you take. This prevents you from repeating unnecessary steps and gives you a semblance of control over the process.

How to Prevent Account Hijacking

You can take steps to prevent account hijacking from occurring in the first place (or again). Considering how easy identity theft is, the primary goal is to put additional barriers in place. Thankfully, the four major carriers do have options. Unfortunately, while Sprint and Verizon make that extra security a requirement for all new customers, AT&T and T-Mobile do not.

If you're a Verizon customer, you should have set up a four-digit account PIN when you started the service. If you didn't, or you forgot your PIN, go to the company's PIN FAQ page, and click on the "Change Account PIN" link. Log in with your Verizon account when prompted.

Sprint also requires a PIN as part of a customer's account setup, so if you're with Sprint, you should already have one. Sprint also requires a security question as a backup and lets you pick from a list. Try to pick a question that can't easily be found in a Google search. If you forgot your PIN, you can sign in to your online account and change it in the Security & Preferences section.

AT&T customers aren't required to set a PIN, but you should. You'll need to log into AT&T's online portal. Look for two options: Get a new passcode and Manage extra security. You should go through both of these processes. Manage extra security simply tells AT&T to ask for your passcode in more situations, like managing your account in a retail store.

By default, T-Mobile asks account verification questions to determine identity. You can set up a PIN to use instead, but the only way to do so is to call them. From a T-Mobile phone, you can use 611. T-Mobile has two options: an account security PIN and a port out PIN. They protect different things, so you might want to set both.

If you're using a service other than the four major carriers, you should check its support site or call customer service to find out what security options you can set up, and how to add them.

Once you have your PINs set, it wouldn't hurt to call back in a day or two and verify that they ask for it. The process is straightforward, and you probably won't run into any issues. Peace of mind and a little practice using your new PIN is worth the time spent—especially if you discover something did go wrong, and your carrier didn't set your PIN correctly.