The Gigabyte Gazette

The Monthly Newsletter

of the

Sun City Summerlin Computer Club

https://www.scscc.club

January, 2023

Table of Contents

President's Message 3
General Membership Meeting 4
SCSCC Board of Directors Actions 4
January 2023 Printable Calendars 4
Submissions Welcome 5
Welcome New Members 5
Special Interest Groups and Kaffee Klatches 6
Seminar and Q&A Offerings 8
Tom's Tech-Notes 10
Kretchmar's Korner 15
APCUG Guest Article 18
Lab Monitor Schedule 20

Issue Contributors

Tom Burt ***Peggy Cushman***

Kathy Kirby ***David Kretchmar***

Jeff Wilkinson ***Jim Cerny***

President's Message

Happy New Year

by Jeff Wilkinson

As we begin a new year after a busy and enjoyable holiday season I am looking forward to offerings which serve all our club members in their own unique ways.

Our usual classes, SIGs and support and repair sessions will continue, and we hope to expand even more with greater participation of our members. Is there some subject you would like to learn more about, a troublesome setting on your device, a question about a planned purchase? We can help. Are you overflowing with information that would be useful to your fellow members? We need you! Can you offer an informative session live or via Zoom or even a full-featured class with presentation notes? Give me a call, 702 527 4056, or email myself or Tom Burt, Education Programs Director. Let's talk!

I've been thinking about the recurring subject of video cameras and doorbells for the home. There's need for an informative session of the pros and cons of available devices, associated recurring costs, in-home hardware needed, HOA requirements, mounting location etc. A seemingly simple subject can quickly become very involved. This reminds us to ask a few very important questions before committing. Anyone have some expertise to volunteer?

So, you can see, the New Year holds much promise for our club and opportunity for our over 570 members to get involved! Please consider your options for the New Year.

Happy New Year!!

Jeff Wilkinson, President
(702) 527-4056 pres.scscc@gmail.com

General Membership Meeting

The January General and Business Meeting will be held at **2 PM on Thursday, January 5** via Zoom webcast only. The program will feature a video presentation by Ron Brown on two-factor authentication.

*For Club information: go to **www.scscc.club**, contact Jeff Wilkinson, President at (702) 527-4056 or email him at **pres.scscc@gmail.com**.*

SCSCC Board of Directors Actions

The Computer Club Board of Directors took the following actions on December 14, 2022

Chuck Hagen made a motion that the **minutes of the November 9, 2022 Board Meeting be approved as submitted.** The motion was seconded by Tom Burt and unanimously approved by the Board.

George Lobue made a **motion** that the **meeting adjourn**. Jeff Wilkinson **seconded** the motion, and it was unanimously **approved** by the Board. The meeting was adjourned at 10:09 AM.

January 2023 Printable Calendars

To view this month's printable classroom and lab calendars, click the following hyperlink:

https://www.scscc.club/Calendars/scscc_calendar_2023-01Jan.pdf

Submissions Welcome

We are always looking for new information to share with our club members. If you have computer or technical information or tips you would like to share with members of the club, send your articles to editor **Tom Burt** at tomburt89134@cox.net. Thank you to everyone for your contributions.

Welcome New Members

The following new 2022 / 2023 members have joined the Computer Club from November 28th to December 30th.

Roger Alberts
Roger Alberts
Donald Butler
Jim Clark
Francis Jones
Constance Kwiatkowski
Josephine Mariani
Timothy Martin
Cas Martinez
Richard Natale
James Schmidt
Melanie Spector
Stephen Yohay
Dale Zeller
Derek Zeller

As of December 30th, the club has 571 paid memberships for 2022 and 226 for 2023.

The Computer Club is now accepting new and renewed memberships for 2023.
Annual dues are $10 per person.

As of December 31, 2021, the club had 618 paid memberships for 2021.
Of those, 17 were new memberships for 2022.

Special Interest Groups and Kaffee Klatches

Special Interest Groups (SIGs) provide a forum for general discussion on a specific computer related subject. Admission to all SIGs is on a first-come, first-seated basis and is subject to the maximum allowed by fire code regulations. <W>, <L>, <M> or <H> indicate whether a SIG would be of interest to a Windows, Linux, MacOS or Hand-held Device user.

Apple iPhone / iPad Lab <M/H> *Live in the Classroom*

Zane Clark 702-332-5747
First Wednesday, 9 a.m. monthly
Next meeting: Wednesday, January 4, 2023

The lab sessions will be in the usual format, one-on-one help with your questions. Come anytime, leave anytime.

Repair SIG <W/L/M> *Live in the Classroom*

Chuck Hagen (702-418-2614)
Every Tuesday, 12:30 p.m. to 3:30 p.m.

The Repair Lab provides **CLUB MEMBERS ONLY** with no-cost assistance for those having upgrades and / or hardware and software problems with their computers. Bring in only your PC tower, your Mac or your laptop and your problems. Our TECH team will give you our best effort. ***Be sure to mark your cables so you can re-connect when you get home***.

Internet Investing <W/M/H> *via Zoom*

Tom Burt (702-341-7095)
3rd Thursday, 9:00 a.m. monthly
Next meeting: Thursday, January 19th

The Internet Investing SIG provides a forum for members interested in using Internet resources for researching and managing investments to meet, discuss, and learn more about the topic. The SIG's target audience is members with intermediate computer skills and investment experience, but all members are welcome.

Kaffee Klatch <W/M/H> *Live in the Classroom and via Zoom*

Jeff Wilkinson (702-527-4056)
Every Tuesday, 8:30 a.m.

This Kaffee Klatch is an open, free-form discussion group for all users, from beginning to advanced. KK discussions are not restricted to any one subject, computer platform or computer-knowledge level but should be computer or technology related. We will try to answer your questions, help you keep your systems updated and provide some useful "tips and tricks."

Windows 10/11 SIG *Live in the Classroom*

Bill Wilkinson (702-233-4977)
First and Third Saturdays at 9:30 a.m.

If you are a novice or near-beginner computer user, or if you just want some refresher information together with a refreshing cup of coffee, then jump-start or recharge your computing knowledge by attending these Windows 10/11 SIG / Q&A sessions. At each session, attendees will explore several topics of interest to beginners and near-beginners. The topics are always announced a couple of days in advance via e-mail to SCSCC members who have subscribed to the club's SCSCCNews mailing list. Each topic is presented in a step-by-step manner and is supported by "how to" notes that can be easily and conveniently downloaded from the SCSCCBKK.org web page. Following each "up front" presentation of one or more topics (approximately 60 minutes in duration), an informal open-ended Question and Answer period takes place for those who wish to participate, listen, reflect, or inquire.

Seminar and Q&A Offerings

The club's educational sessions are being conducted either as Zoom webcasts, live in-person or a hybrid of the two. Check the weekly calendar on the website to see which mode the session is using. Unless explicitly stated, advance registration is not required for these sessions.

Google Sheets – Managing Your Data

Monday, January 16th from 9 to 11 AM
Presenter: Gail Weiss
Location: Classroom Live and Zoom

Happy New Year!

Google Sheets, which is a **FREE** spreadsheet application like Excel, isn't just for number crunching. Whether you want to keep track of a list people (i.e. club membership, friends and family) or keep track of all your worldly possessions (i.e. record or book collection), you can use Sheets to view your data in many different ways. You can filter it, so you see only data that matches specific criteria (i.e. only friends that live in California or only records by a certain performer). Even if you are new to a spreadsheet application or just need a refresher, I will start with the basics and show you how you can use Sheets to keep track of all your data.

As long as you can access the Internet, the files you create with SHEETS will then be automatically saved to your personal GOOGLE DRIVE cloud. You will also be able to save the files to your own device or share them with others.

This class will be held in the Computer Club Classroom, so please bring your own laptops or mobile devices if you want to follow along. For more information about this class or if you have any questions or ideas for future classes, please email me at gmweiss5@gmail.com.

Photoshop Elements – Introduction to Layers

Wednesday, January 25th at 1 PM Live
Presenter: Mary Miles

Mary will introduce the layers features of Adobe Photoshop Elements with some interesting image editing projects.

Tax Preparation Software – Tax Year 2022

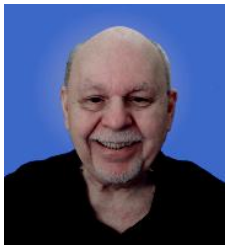
Monday, January 30th at 10:00 AM *via Zoom*
Presenter: Tom Burt

Two of the most popular programs for preparing your personal income tax return are **H&R Block** and **Turbo Tax**. You can run these programs on your PC or Mac or you can work with the online versions. Purchase one of these software programs, install it on your PC (or go to the maker's website) and answer the step-by-step questions that are presented to you. When you've finished, either program will provide you with a finished tax return ready for filing. You can even choose to file your return electronically! Happily, for 2022 the tax law changes for individuals were few and minor.

In this year's seminar we will discuss both programs briefly and then do a demonstration of the excellent H&R Block Deluxe program. We will create a 2022 tax return for a fictitious senior couple who have typical financial transactions such as: wage income or retirement benefits, interest and dividends, social security benefits, capital gains, itemized deductions, required minimum distributions, etc. You may be surprised how easy it is to prepare and file your own tax return. We'll also look at how to set up electronic payments on the IRS web-site.

2022 presentation notes will be available about January 22nd at: http://www.scscc.club/smnr.

We will be recording this seminar and posting it to the club website.



Tom's Tech-Notes

Home Router Hygiene

Originally published June, 2019

Introduction

It's the beginning of the new year. I decided to reprise a column I wrote in June 2019 that discusses key things you need to do to make sure your home router is as secure and reliable as possible.

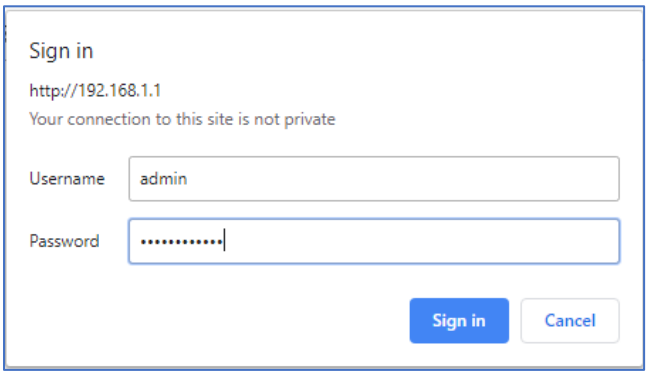
All network traffic inside your home and all external Internet traffic flows through your home router. An insecure router can provide an entry point for hackers to break into your home network and also to monitor network data traffic, hoping to capture personal and financial information that can be used to steal your identity and assets.

In the following, we'll talk about a few important things you can do to make your home router as secure as possible. My examples and screen shots are from a late-model Netgear AC1750 R6400 router. If you have a different make (Linksys, DLink, Asus, TP-Link, …) your router's screens and settings are likely a bit different, but the key settings should still be available.

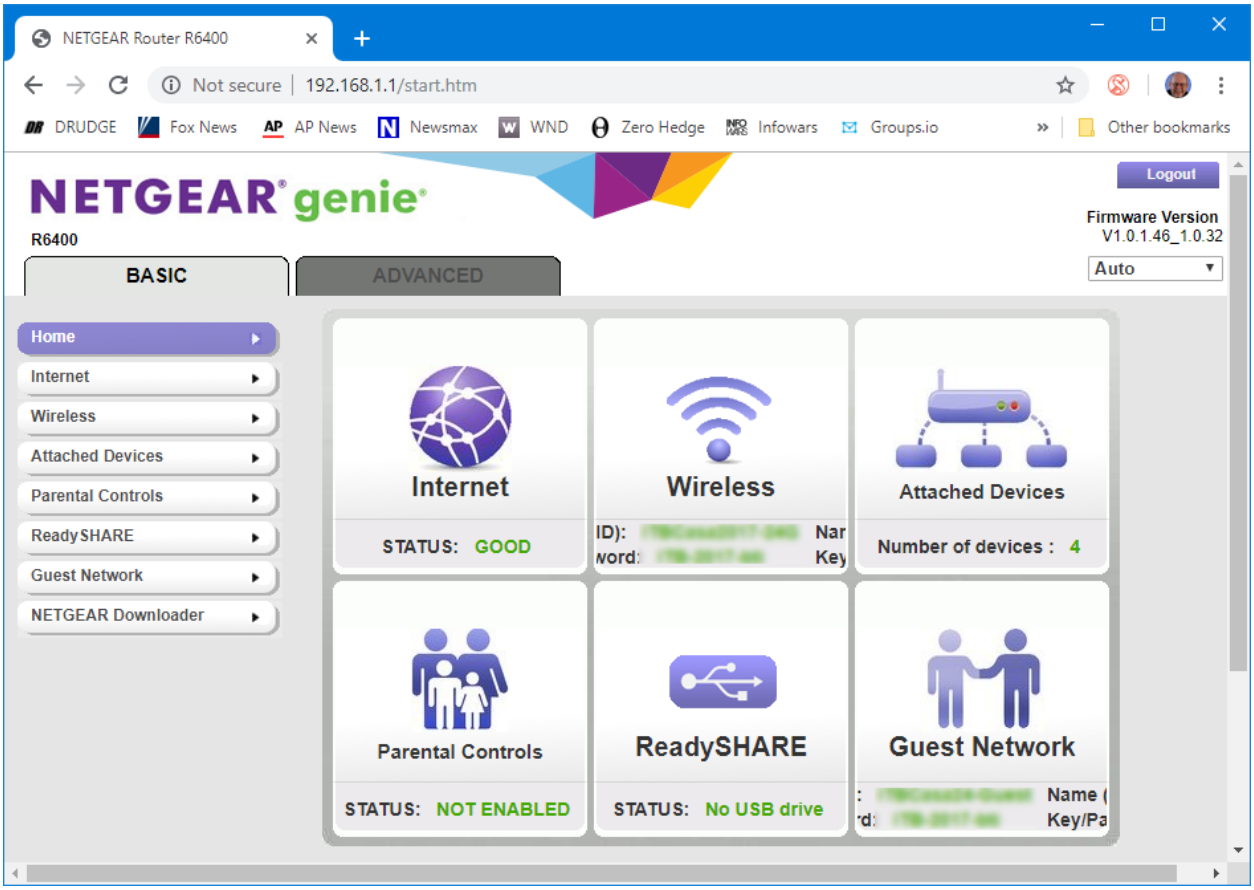
Logging in to Your Router

Modern routers all have a built-in Settings interface, implemented as a set of web pages. To get to the Settings interface, start your web browser on a device connected to the network **via an ethernet wired cable**. In your browser's address box, enter the internal IP address of your router. To find this in Windows, click the Start icon, then click the Settings gear icon. Click Network & Internet > Status > View Your Network Properties. Your router's internal IP address is the **Default Gateway** address. For my router, it's **192.168.1.1**.

After entering 192.168.1.1 into the browser's address box, the login screen appears:



Enter the Username (“admin”) and Password values and click the Sign in button. The router’s main settings screen will appear in your browser.



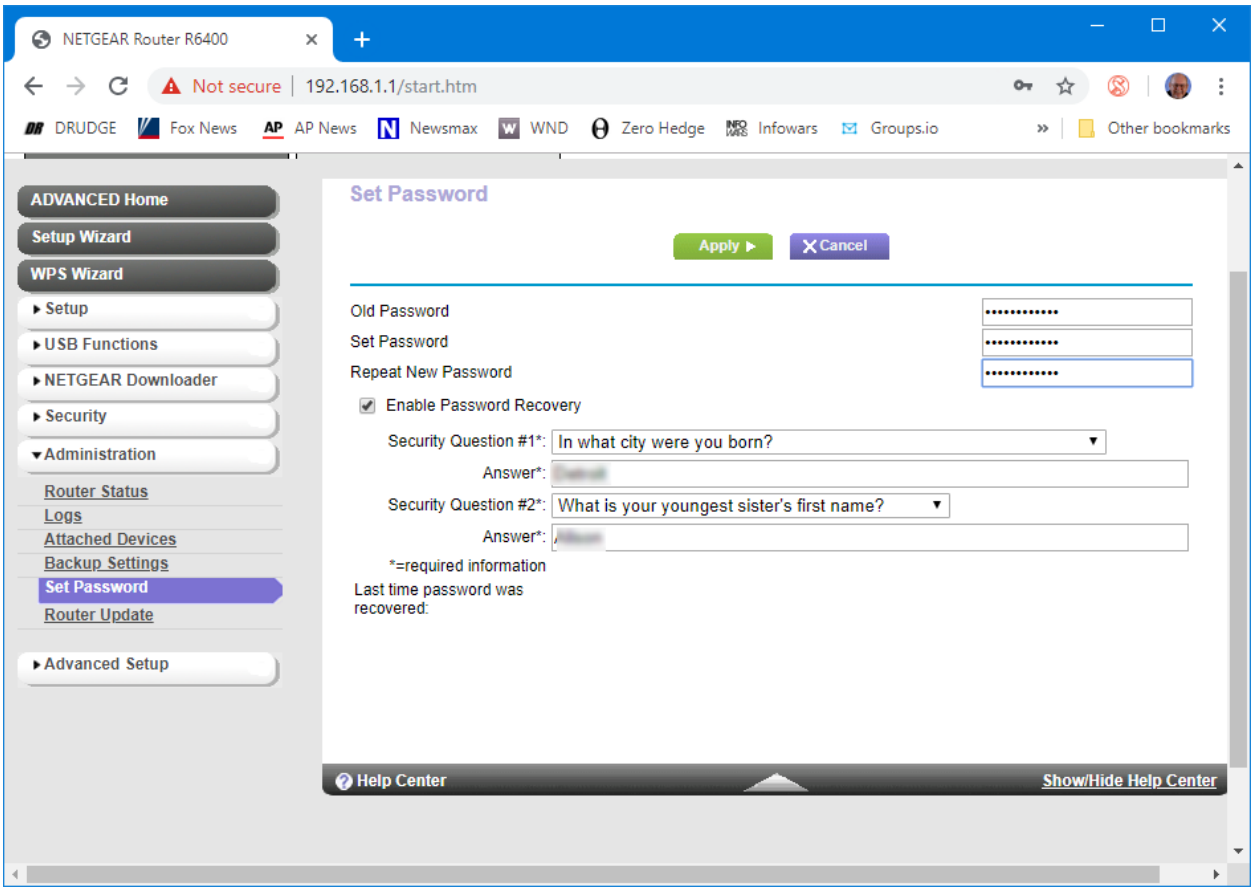
Netgear Router Main Screen – Dashboard

The buttons along the left side, when clicked, lead to various screens showing specific settings you can review or change. Notice that there are a Basic and an Advanced tab.

Setting an Administrator Username and Password

The first thing to do is check and modify the default Administrator Username and Password. On my Netgear, this setting is found on the Advanced tab in the Administration section. Click the Set Password link to display a “set password” dialog (see below). Enter the old password and then enter the new password twice. The Netgear router does not offer an option to change the Username; it is always “admin”. Consequently, use a very strong password (long, mixed upper/lower case letters, digits, special characters). Make sure you write this down and store it in a safe place or in your password manager software’s vault.

You may want to enable the Password Recovery feature, which has two security questions and answers. The final screen appears below. Click the Apply button to save the changes.



Netgear Router – Set Administrator Password Screen

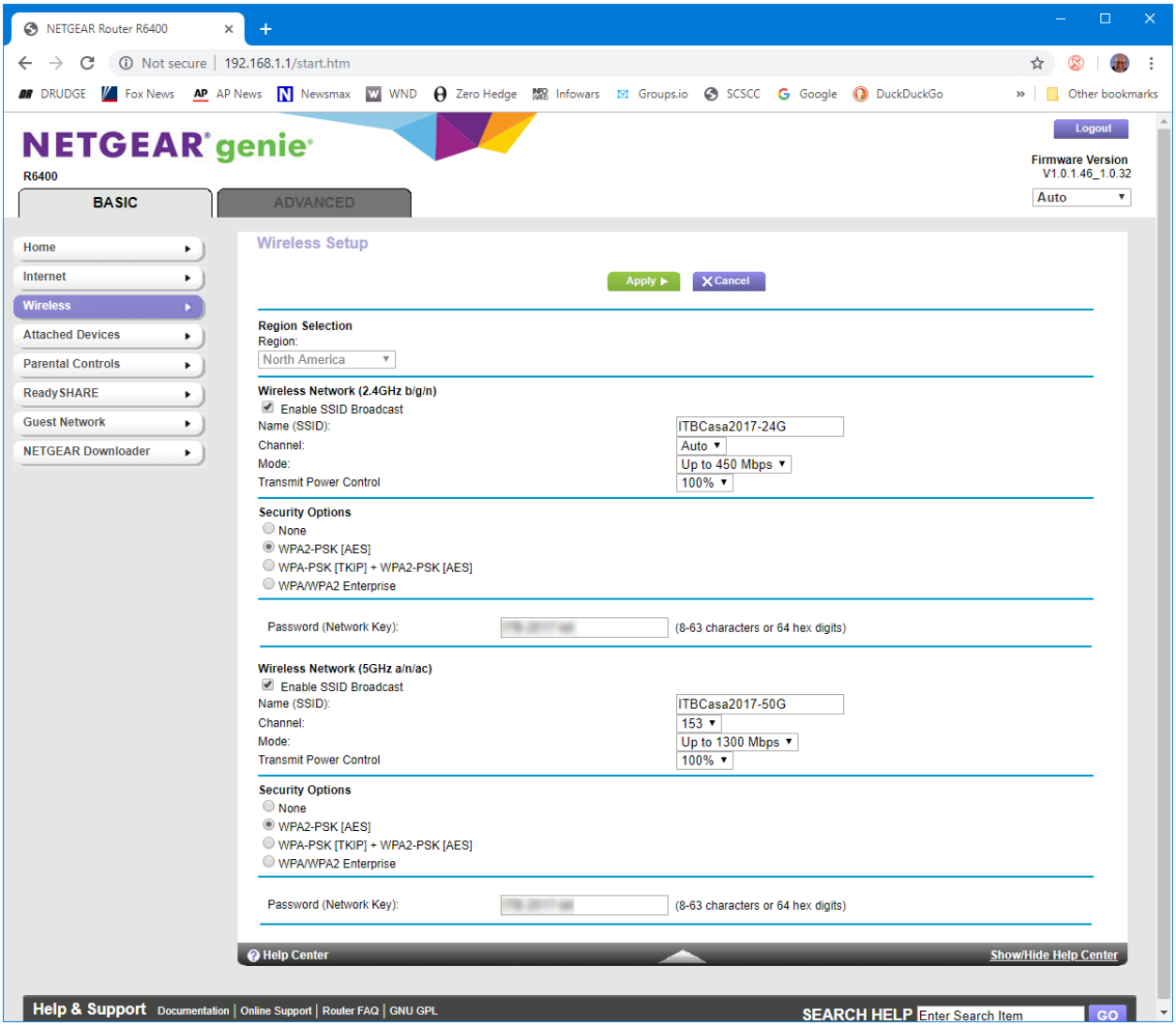
Setting a Wireless Encryption Password

The wireless data traffic between your router and connected wireless devices is carried via radio waves. These have a range of several hundred feet and so can be detected by any nearby wireless device. Electronic eavesdropping is thus very easy. To secure your wireless data traffic, it is critical to set up a wireless encryption password. Once this is done, only devices that know the encryption password can connect to your router. All of the wireless data traffic is encrypted using a very strong key derived from the password. This makes eavesdropping by outsiders effectively impossible.

The settings screen for wireless encryption is found on the Basic tab. Click the **Wireless** button to display the Wireless Setup screen. It has a variety of settings (see below). Since my router has dual bands (2.4 GHz and 5 GHz), there are separate settings for each band. Late-model routers also support a 6 GHz band.

The key things to set up are the **SSID** (a name for your network), to turn on WPA2-PSK (WPA2 with private shared key) encryption and to set the actual encryption password. For the **SSID**, choose a name that is meaningful to you, but doesn't directly disclose your identity. For example, I chose "ITBCasa2017-24G" for the 2.4GHz band. For the **passwords**, I chose a 12-character string of mixed upper / lower case letters and digits (mine are blurred in the screen shot) for both bands. A connecting wireless device only has to enter the encryption password

once; the device will remember the password for future connections. When the settings have been entered, click the Apply button. Make sure to write down the encryption password.



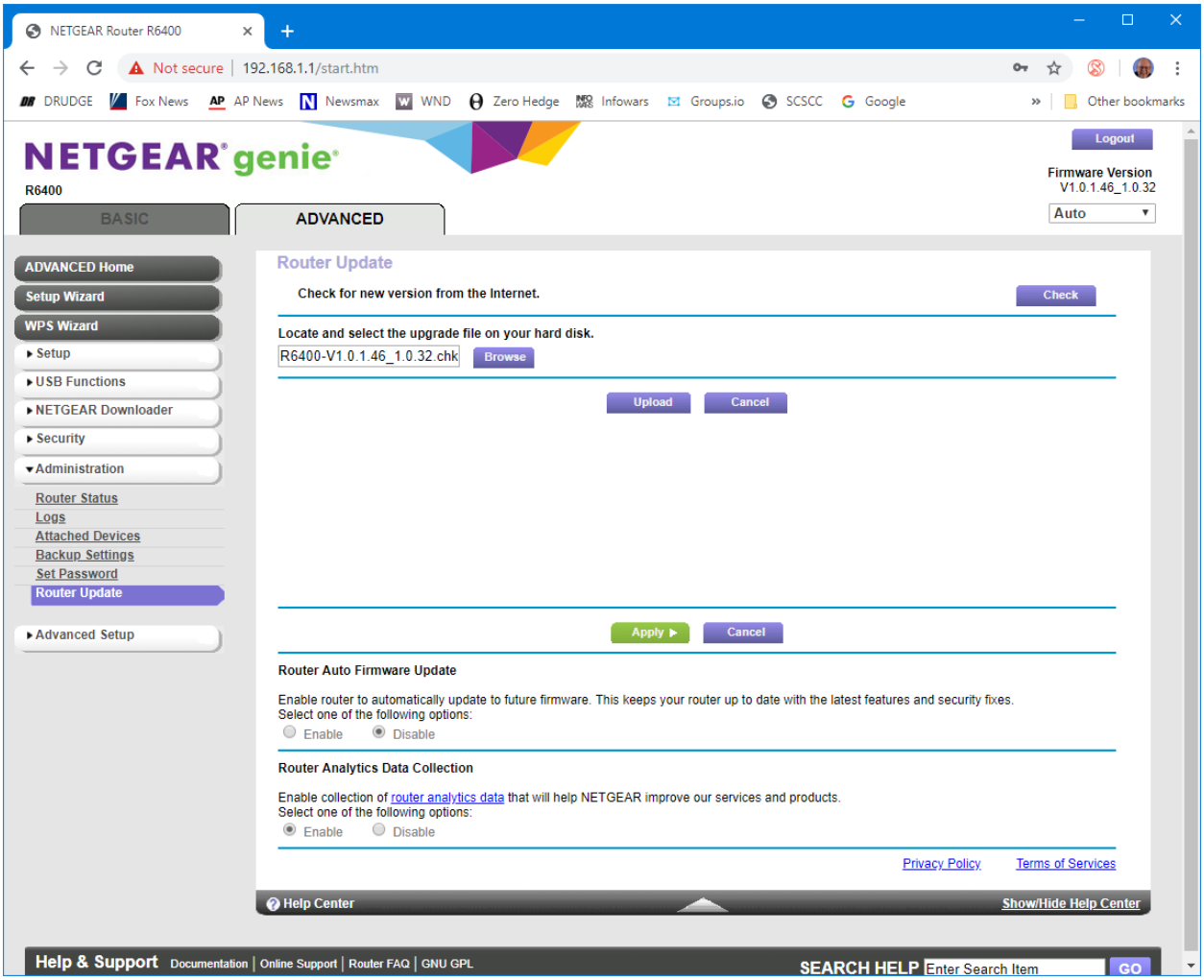
Netgear Router – Wireless Setup Screen

Updating Your Router's Firmware

Your router is actually a specialized computer, running built-in software (firmware) stored in flash memory. Occasionally, bugs and security flaws are found in the firmware that need to be patched to keep your router secure from outside hackers. Your router vendor's support website will offer the latest firmware as a file you can download to your PC or even directly to your router. Once you have the latest firmware file, the Settings interface can update the router's internal firmware.

On my Netgear router, the firmware update screen is found on the Advanced tab; click the Router Update button to display the Router Update screen. If an update is available, this screen will normally display a notice to that effect. You can click the **Check** button to have the router check the Netgear support website for a newer version of the firmware. I prefer to use my web browser to download the new firmware file to a folder on my PC and then, in Router Update, I

click the **Browse** button to select that firmware file. I then click the **Upload** button to install the new firmware. **Be sure you're doing this via a *wired* ethernet connection to the router.**



Netgear Router – Router Update Screen

The firmware update takes about 5 minutes. Update progress is displayed with a progress bar. At the end, the router restarts. When that is finished, you can log in to the router and check the firmware version number to confirm the update succeeded.

Other Actions

As you browse around your router's Settings interface, you'll see many other things you can adjust. We've only covered a few of the key basics here.

I recommend that about once a year you take the time to check and update your router, including changing the administrator password and the encryption password. Also, it's a good idea to occasionally (maybe once a month) power your router off and back on. This gets rid of any malware that might have broken in as well as flushing out stale data and any other corruption.

Kretchmar's Korner

'Tis the Season for Fraud

David Kretchmar, Computer Technician

We have all received emails that appear to come from a bank or other online service requesting that we provide account credentials. You might have been asked to provide extremely personal information including account and credit card numbers and passwords. This is a standard phishing technique, and the fake sender is oddly asking for information that entity should already have. Recently we've seen once again phishing lures are mutating like the COVID-19 virus and they're becoming more difficult to recognize.

> ***"If you can't spot a phishing email, you could be the next victim."***

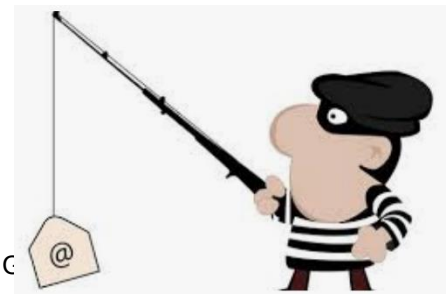
Phishing is a form of social engineering email attack in which the sender tries to gain access to login credentials, to get confidential information, or to deliver a virus. This is accomplished by tricking humans like you and me.

Scammers know that there's a good chance that any message will be scanned for malicious content by the security software of your browser and mail provider. Google, Edge, and most other browsers are decent about stopping known spam, but plenty still gets through. Roughly 15 billion spam (unwanted) emails make their way across the internet every day, which means that filters are overworked and are liable to permit phishing attack emails to slip through to your inbox.

Fraudsters waste no time in trying to profit from the uncertainty and fear that are always a part of our world. In 2023 there is great concern about inflation, falling stocks and cryptocurrencies, and war. These themes are ripe for spam, spreading malware, and phishing for sensitive information.

I have read that amazingly 30% of phishing emails are opened by their targets and over 90% of security breaches in businesses are a result of phishing attacks. If you can't spot a phishing email, you could be the next victim.

So how do you recognize suspicious emails?



The sender's email address is the first place to look. If it looks "funny" or unfamiliar be careful with that message. You can check the email address by just looking at or hovering your mouse over the 'from' address *but don't click*. Scammers' email addresses may appear to be anonymous or

very generic names with many numbers. Sometimes the sender's email address will not match the sender's name or the body of the message.

Receiving emails about a problem with your account from financial institutions with whom you have no relationship is obviously a laughable tell. But if you do get an email claiming to be from your bank, closely review the email address. The email address is sometimes the only sign of a scam, due to how professional the messages look. If you feel the email might be legitimate, check your account the way you would normally access it (never a link provided in the email).

Keep in mind that any big outfit is going to own their own domain and have at least a partially eponymous address; for instance, you contact PayPal or Amazon at an address that includes paypal.com or Amazon.com.

Be suspicious of attached files or unfamiliar links

Cyber criminals' email might contain malware or send you to a malicious web destination. If you are at all suspicious, don't click. Legitimate service providers don't send messages requesting you to log in via an embedded link. Also pay special attention to attached files; once they are opened, these attachments can give someone else control over your computer. They can then initiate attacks on other computers, including by sending spam (often infected) to every contact in your address book. Sadly, I have been the victim (many years ago) of that kind of attack.

Watch for poor English

Poor grammar or words used in an unusual way is a possible indication of phishing. Always be suspicious. Looking for unusual language and vocabulary, or misspelled words can help prevent you from becoming the next victim. Poor spelling and other grammar mistakes are common with phishing emails that have been translated from other languages. This kind of clue is less common today because the quality of social engineering has improved, so you are likely to receive a more professional presentation. Another thing that can signal an attempted attack is generic greetings such as "Dear recipient" (who else would be receiving it?) or " Dear friend" (trust me, they are NOT your friend).

There's sometimes a subtle purpose behind misspellings and poor sentence structure. Cyber criminals most successfully prey on uneducated computer users, knowing they are less observant and therefore easier targets.

Is it too good to be true or is it frightening?

Social engineering focuses on two human weaknesses, fear and greed. Does the email promise you a windfall of cash? Does it suggest you inherited a fortune or will be paid a fortune to help someone move money out of their country? Walmart, Target, Costco or whoever are not going to give you $75 just for taking a moment to complete a simple survey. Here's an idea: Google for the same message, or a key phrase from that message. (highlight, right click, search Google). You'll often see that many other people have received the same or similar fraudulent message.

Would be cyber criminals using social engineering methods are very opportunistic. For example, this time of the year the names of shopping websites such as Amazon and Mayfair are used in sending out millions of emails claiming issues with your account or recent order and asking for personal information. They know consumers are most likely to have made purchases this time of the year.

The scammer wants to panic you into doing something. Don't be threatened by an email. Does the message urgently ask for help or otherwise appeal to your emotions? These are common techniques. Do not respond to an email threatening to suspend your account if you do not answer in a short time.

Homoglyph attacks

Homoglyph attacks rely on replacing characters in addresses with ones that look similar, or are the same, but belong to different alphabets. These attacks are extremely dangerous for users because there is a very limited chance of detecting the trick. In a recent attack on PayPal users the sending address appeared to contain the "correct letters" taken from our Latin alphabet – with two exceptions. The attackers replaced both instances of the letter P with a "P" look-alike letter, but from a different alphabet. This "P" look-alike letter was taken from the Russian alphabet, where it is equivalent to the letter R. With this kind of attack, you are dependent on the other clues discussed in this article to protect yourself.

But all is not gloom and doom. You can become your strongest protection against phishing attacks by using common sense and being suspicious of every request you receive for personal information.

APCUG Guest Article

"Default" apps or programs in Windows

By Jim Cerny, Vice President, Education Chair, and Forums Coordinator
Sarasota Technology Users Group
https://thestug.org/ jimcerny123 (at) gmail.com

Most of us know what "default" means when talking about computers or technology. But in case you forgot, "default" means: "This is what you get until you change it to something else."

Computer technology is full of defaults (you may have also heard the term "default settings"). The best way to understand this concept is to use an example. Suppose you are writing a document using Microsoft Word (or some other word processor app); you can start typing words in your document immediately without selecting the FONT or FONT SIZE first. That's because the app has a default font setting (such as "Times New Roman" in the font box and "12" in the font size box). Yes, you can go to those boxes and pick any other font size you want, but the app already starts with something in the box. That's the default. Other examples in everyday life are thermometers using Fahrenheit, but you can change it to Centigrade, or your speedometer from miles-per-hour to kilometers-per-hour. If you don't like the default setting, change it to something else.

Let's go one step further and discuss using that essential Windows app called "File Explorer." With File Explorer, you can find any file on your computer. And when you find the file you want, you can OPEN that file by double-clicking on the file name. Of course, there are many different types of files – photo files, document files, spreadsheet files, and many more. So, when you double-click on a file name in File Explorer, Windows uses the DEFAULT app to open that file. Let's take a photo file as an example. In File Explorer, if I double-click on a photo file (a file type of ".jpg"), it will open the photo in the Windows Photo Viewer app, and I can see the photo. But if I want to open that photo in a different app, say the Windows Paint app, I have to open that app first and use the app to open the photo file.

It turns out that your Windows computer already has selected specific apps for many file types to use as the default apps. And it's no surprise that your default apps are Windows or Microsoft apps.

Here is one more example. If you click on a web page link, your computer will open and use the default web browser to go to that web page, probably Microsoft Edge. But you can change your default web browser to Google Chrome, Safari, Firefox, or any other browser you want.

(Ed note … I added some material to the following paragraph to discuss how to set default programs in Windows 11. Jim's original article referenced only Windows 10. … Tom Burt)

To do this, click on the Windows Start button in the far bottom left or center corner of your taskbar, choose Settings (gear icon), choose Apps and finally select "Default apps". In Windows 10 click on the Web browser setting to see a list of the web browser apps you have and click on

the one you want as your new default browser. In Windows 11, you will see a list of apps. Microsoft Edge and any other installed web browsers will appear in the list. Click on the browser you want to make the default. A list of web file types will appear below a panel that says “Make <browser name> your default browser” and has a button “Set default”. Click that button to make your preferred browser the default program to open web files and hyperlinks.

This procedure is how to change ANY default app on your computer to a different one. You can also get to the “default apps” area through your computer “settings” or “control panel.” In addition, you can change the default app used for different file types. It is not difficult to do this. For example, to learn how, use Google search on the internet and enter “How do I change my default app for .jpg file types” or anything else.

The benefit of knowing about default apps is that you will understand why a specific app is used when you click on something to open it. This also explains the question you sometimes get “Select the app you want to use to open this file,” which could mean you may not have an app that can open it.

The best way to make sure you use your preferred app to open a file is to open that app first and use the app’s “open file” action (menu, button or link) to select the desired file. Unfortunately, the default is not the de-fault of your computer!

Lab Monitor Schedule

The Open Lab session is held once per week: 9 am to noon on Saturdays.

January	Monitor Schedule
Jeff Southwell Linda Muench	Saturday 1/7/2023
Fred Cohen Linda Muench	Saturday 1/14/2023
John Zuzich Raymond Pun	Saturday 1/21/2023
Linda Muench Gail Weiss	Saturday 1/28/2023