



---

# Invitation Models and Best Practices

# Contents

- Invitation Models .....2
  - Benefits and Risks of Each Invitation Model .....3
  - Invite Only and Invite + Realm Account Sign Up Requests Models.....4
  - Open Invitation Model.....5
  - What Can New Registrants See?.....7
  - Updating Privacy Settings for Someone Else .....8
  - View/Edit Someone's Privacy Settings .....9
  - Check Your Overview Dashboards..... 10
  - Communicate Privacy Settings ..... 12
  - Set Your Privacy Preferences ..... 13
  - Understanding Privacy Settings..... 14
  - Tips for Using Realm Account Sign Up Requests Safely..... 15
  - Security Takes All of Us..... 17

# Invitation Models

Should you encourage congregants to sign up for Realm on your website or should you send invitations? This article explains each invitation model.

In order to take full advantage of all that Realm has to offer, you'll want to make it as easy as possible for congregants to find small groups, communicate with each other, access personal giving history, or register for events. But it's also important to balance this transparency with privacy concerns and understand the benefits and risks of both invitation models. You'll need to decide if congregants will be allowed to register for events and/or anonymously give online to your church.

**?** **TIP:** Keep in mind that invitation models are not "set-it-and-forget it". As an administrator, you can easily change your invitation model to serve various strategies or goals, but they do come with [benefits and risks](#).

There are three types of invitation models. By default, all accounts are set to the invite only model when you first purchase or convert to Realm.

To see what invitation model you're using, go to [Settings](#)→[Security & Privacy](#) and click the [Invitation Model](#) tab. You can select from the invitation model types:

- **Invite Only** - Individuals can only be invited by the church. They can not send a request to create a Realm account.
- **Invite + Realm Account Sign Up Requests** - Individuals can be invited by the church and can send a request to create a Realm account. Administrators must approve or decline the request.
- **Open** - Anyone can automatically sign up and create a Realm account.

## Benefits and Risks of Each Invitation Model

| Feature  | Open Invitation | Invite Only | Invite + Realm Account Sign Up Requests |
|--|-----------------|-------------|---|
| Reduce possibility of duplicate records  |                 | ✓           | ✓                                       |
| Church controls who receives an invitation   |                 | ✓           | ✓                                       |
| People join without an invitation being sent from someone at the church                      | ✓               |             |   |
| People can send a request for a new account, which must be approved by someone at the church |                 |             | ✓                                       |
| Reduced need to monitor the Overview dashboard   |                 | ✓           | ✓                                       |
| Greater responsibility on church leadership to educate congregants about privacy settings    | ✓               |             |   |
| Best used for campaigns, promotions, or limited occasions                                    | ✓               |             |   |

## Invite Only and Invite + Realm Account Sign Up Requests Models

Adding people by invite only is the most secure method of inviting people to use Realm.

The Invite Only model provides you with the most oversight. With invite only, congregants can join Realm only by invitation sent from authorized users. With Invite + Realm Account Sign Up Requests, individuals can also send a request to create a new account.

An administrator must approve or decline congregant profile requests from the [Task](#) page. Invite only is the default setting, and we recommend that you keep this setting until you have the opportunity to educate your congregants about privacy settings.

Since only users with a login can enter, any new users of your site must first be issued an invitation. To invite congregants into Realm, an administrator, a group leader, or a servant team leader with the correct permissions will need to send invitations. There are a number of ways to send invitations.

- When adding a new profile
- From reporting dashboards
- From pathways
- Via groups
- By query and mass invitation

## Open Invitation Model

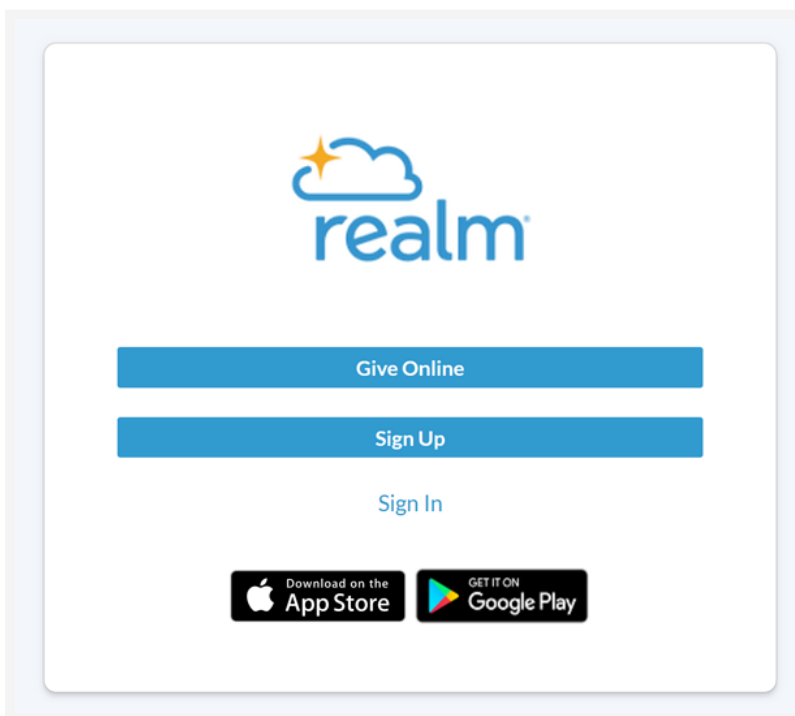
Before choosing an open invitation model, be sure you understand the challenges with this method of inviting people into Realm.

The Open invitation model allows visitors to your website or visitors with your customized Realm URL (onrealm.org/yourchurchnamehere) a way to create a login on their own. When using this model, you do not need to invite people in, but you do have a responsibility to educate your flock about their personal privacy settings. You'll also want to monitor your activity dashboard on a daily basis to see who has signed up.

**⚠ CAUTION:** Before choosing this model, we recommend that offices thoroughly understand their responsibilities in protecting the privacy of their office data by [understanding how member's information can be misused](#). We also recommend this option be used for limited periods of time.

Because new registrants can view the online directory (including non-private profile information), we recommend using the open invitation model for a limited period of time, such as when you first roll out Realm, a specific promotion period, or season when you want to encourage people to sign up instead of sending out invitations. See [What Can New Registrants See?](#)

- To check what invitation-model you're using, go to [Settings](#)→[Security & Privacy](#) and click the [Invitation Model](#) tab. If you have selected the open invitation model, this means the [Sign Up](#) button on your log in page is visible. Remember, you can change your invitation model at any time.



# Do I Need to Use the Open Invitation Model for Online Giving Forms or Event Registration?

The answer to this question is..."It depends on your goal." There are options for encouraging non-registered users to give or sign up to attend an event. If that is your goal, the invite only model will likely be sufficient. If, however, your goal is to encourage people to also create an account in Realm, we suggest you educate your congregants about privacy settings, turn the open invitation model on and then monitor new registrations daily.

1. To receive online donations, you can use either invitation model along with giving forms published to your web page. See help for "Online Giving Forms". The giving form collects enough information that a non-registered user can give one time or recurring gifts online. If you want congregants to manage their recurring gifts, you can send them an invitation.
  - a. Invite only model - Giving forms used with the invite only model DO NOT give a donor the ability to create an account.
  - b. Open invitation model - Giving forms DO give the donor the ability to create an account.
2. Similarly, you can create a URL that allows people without logins to register and pay for events through your website. Search help for "Share a Registration Event Link."
  - a. Invite only model - You can register for an event and you can make a partial or full payment for the event without creating an account.
  - b. Open invitation model - Functions the same as the invite only model. You can register for an event and make a partial or full payment for the event, but you cannot create an account during the registration process.

## What Can New Registrants See?

This article explains what new account holders can see right after they create an account in Realm and before they are added to groups other than the system groups.

When congregants first register for an account, they may be placed in one or more system groups, depending on their profile. The important thing to remember is that if using the [open invitation model](#), everyone who registers via the [Sign Up](#) link is placed in your office group. All users in these system groups can see:


- The online directory. For specifics, search help for "Privacy and the Online Directory". We strongly recommend that you ask permission before including a congregant in the online directory.
- Communication (inbox and chat) sent to any of the system groups. (In most cases, this is the office-wide group.)
- Events published to the office group. For specifics, search help for "System Groups".
- Their personal giving history.
- A list of groups. Only an administrator can add a new user to a custom group, such as Spiritual Formation Class, Sunday School Class, or Youth Group.

Because of this, office leadership should explain or demonstrate to congregants how to adjust privacy settings. For more information, see [Communicate Privacy Settings](#).

The screenshot shows a directory interface with a teal header labeled "Directory". Below the header is a search bar with a magnifying glass icon and the text "Search...". Below the search bar are four user profiles, each with a profile picture, name, phone number, and email address. Two profiles have callouts indicating their privacy settings:

- Jane Aaron**: (555) 555-1234, janeaaron@example.org. Callout: "Jane's contact information is set to 'anyone can see'".
- Amber Harris**: Callout: "Amber's contact information is limited to specific groups".
- Derek Martin**: (555) 555-3456, derekmartin@example.org.
- Michelle Martin**: (555) 555-3456, michellemartin@example.org.



 **TIP:** You can view system groups, as well as all other groups on the Manage Groups page. In the top-left corner, click your ministry hub then [Realm](#). Then click [Groups](#)→[Ministry Areas](#). Then expand the [System Groups](#) ministry area.

## Updating Privacy Settings for Someone Else

Registered users of your Realm site can view and register their privacy settings. But there might be times when you need to do it for them.

When you change an individual's privacy settings, he or she will be notified automatically by email. Changes are also recorded in the Customization History section of the Privacy page. In order to provide the most current information, the Customization History section displays privacy changes from the past 12 months.

When you change someone's profile privacy, Realm automatically sends them an email listing the new settings. (A popup message will remind you of this.)

But there is an exception to this safeguard. No email is sent if:

- the owner of the profile does not have an email on file
- the profile has not been opted in to the online directory

# View/Edit Someone's Privacy Settings

Registered users of your Realm site can view and manage their own privacy settings. But there might be times when you need to do it for them.

## Before you begin

To view a user's privacy settings, you must have the [Edit Individual People, Personnel, Church, and Org/Business Profiles](#) permission set to **Allow** in your list of responsibilities. If an administrator marks information, such as emails or phone numbers, as visible to users, the [View Details for Individuals People, Personnel, Church, and Org/Business Profiles](#) permission must be set to **Allow** in order for the user to view the information.

For more information, see [Responsibilities](#).

## Procedure

1 **Locate** and open the user's profile.

2 Click to the privacy icon  **Privacy**.

3 A detailed list of settings opens.

For people without a login, the check box **Opt in to Online Directory** is visible. If selected, this individual's profile is searchable by others in Realm, even if he or she never creates a login.

4 Select one of the options to apply that setting to all information on the profile, or click **Custom Privacy** to select a setting for each field.

5 Other members in this person's family display on the left. Click each family member's name, and select a privacy option.

6 Click **Save**.

## Check Your Overview Dashboards

When using the open-invitation model, it's very important that you monitor your overview dashboards for new registrations and unusual activity.

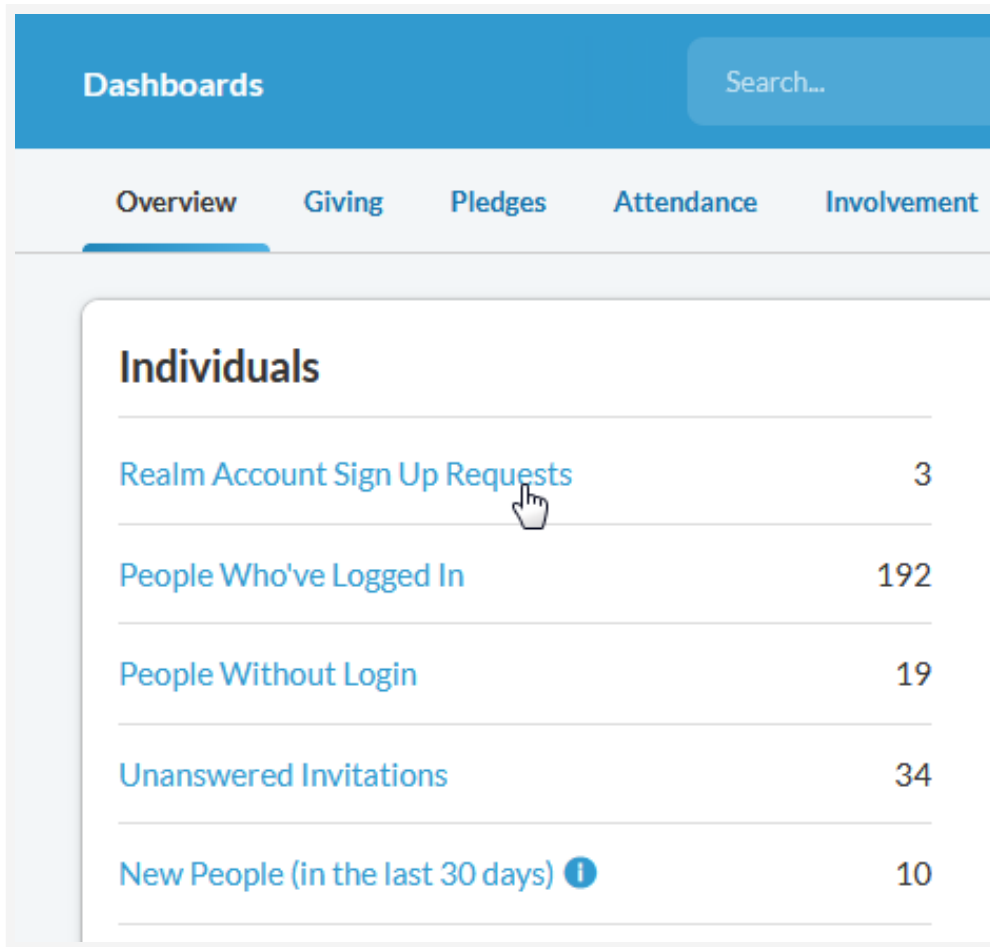
You should monitor registration and login activity daily. Filter the list to see individuals who added themselves. Look for names you do not recognize or strange email addresses. If you see anything suspicious, remove the registrant and consider turning off the open-invitation model until you can investigate further.

### TIP:

It takes all of us being continually vigilant when it comes to online security and privacy. Criminals will do just about anything to obtain verified email addresses with the intent of conning sympathetic people out of their hard-earned cash.

A common tactic, for example, is to break into an email server to obtain large lists of email addresses or cell phone numbers, or to access and hold office data hostage for a sum of money. Another potential tactic is registering for a login in order to access personal contact information. These miscreants then send emails or texts that appear to come from the pastor of the church, but are, in fact sent from servers that usually reside in foreign countries. These emails often include gift cards scams or other fake requests for financial assistance.

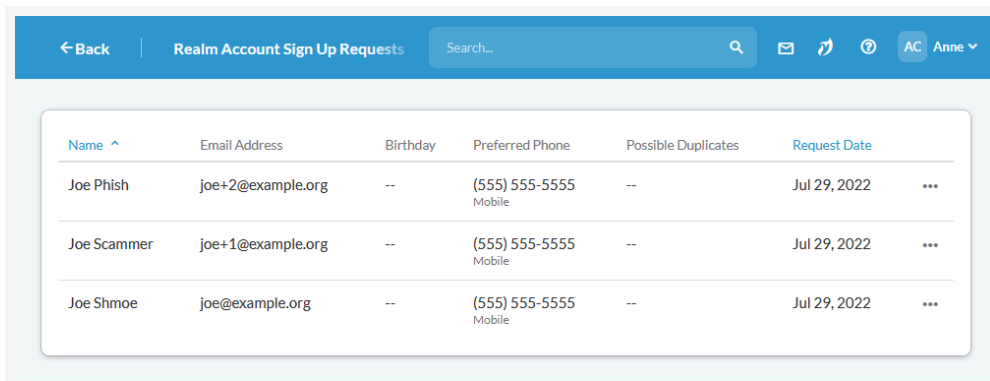
To read more, see [Security Takes All of Us](#).



The screenshot shows a dashboard with a blue header containing the word "Dashboards" and a search bar. Below the header are navigation tabs: "Overview", "Giving", "Pledges", "Attendance", and "Involvement". The "Overview" tab is selected. The main content area is titled "Individuals" and contains a list of categories with counts:

| Category   | Count |
|--|-------|
| <a href="#">Realm Account Sign Up Requests</a>   | 3     |
| <a href="#">People Who've Logged In</a>          | 192   |
| <a href="#">People Without Login</a>             | 19    |
| <a href="#">Unanswered Invitations</a>           | 34    |
| <a href="#">New People (in the last 30 days)</a> | 10    |

Click any of the blue categories of individuals to view, filter, or sort details.



The screenshot shows the "Realm Account Sign Up Requests" page. The header includes a back arrow, the page title, a search bar, and user information "AC Anne". The main content is a table with the following data:

| Name ^      | Email Address     | Birthday | Preferred Phone          | Possible Duplicates | Request Date |     |
|-------------|-------------------|----------|--------------------------|---------------------|--------------|-----|
| Joe Phish   | joe+2@example.org | --       | (555) 555-5555<br>Mobile | --                  | Jul 29, 2022 | ... |
| Joe Scammer | joe+1@example.org | --       | (555) 555-5555<br>Mobile | --                  | Jul 29, 2022 | ... |
| Joe Shmoe   | joe@example.org   | --       | (555) 555-5555<br>Mobile | --                  | Jul 29, 2022 | ... |

## Communicate Privacy Settings

Here are resources you can use to help educate congregants about privacy settings and the online directory.

Many people regard the church as a safe haven. In fact, in a broken world, they desperately need the church to be a safe place for them and their family. While congregants may rarely consider the online tools and data their churches and denominational offices use on a daily basis, we do and we know you do as well! For this reason, ACST dedicates an abundance of time and resources to protecting the privacy and security of Realm data. And we strongly recommend transparency with congregants and parishioners when it comes to protecting them and their privacy.

We encourage you to educate and communicate with your staff and congregants on the importance of managing privacy settings in Realm. Share your internal policies for safeguarding data and vulnerable members, and make sure people know how you plan to communicate financial needs in your office.

While you'll write a message that suits your particular situation, we provided a sample communication below to get your thoughts flowing around this topic. We'll continue to update the [online resources](#) mentioned in this article as well.

### Sample Email to Congregants

Dear [First Name],

We understand that your online privacy is important to you. For this reason, we'd like to routinely communicate about how we conduct the business of the church. For example, our staff reviews all new Realm registrations, and will work to engage and legitimize all new members with a welcome for the purpose of protecting others. We run annual background checks for anyone directly involved in ministering to children and vulnerable adults. Additionally, we'll never ask you directly for money or gift cards, but instead will ask that you give through various funds set up by the church.


While we want to encourage community, especially among teams and small groups, we recognize that not everyone is comfortable sharing personal information church-wide. Please take a few minutes to sign into Realm and update your privacy settings.

To review your privacy settings, go to [Your URL], and, in the upper-right corner, click [Manage Privacy](#). For your convenience, [here's an explanation of privacy settings](#).

### Online Resources

- [Is your church being Smished in a gift card scam?](#)
- Church Growth Blog: [Information Security and Privacy for Congregants](#)

- Search our [help portal](#) for topics on congregant privacy, passwords, and settings.

🔗 **TIP:** Did you know that you can find help specific to the Realm page you're on? In the upper right corner, click the [Help](#) icon for assistance? 

# Set Your Privacy Preferences

Control who sees your personal information.

## Context

Many find the online directory in Realm invaluable for locating contact information, putting faces with names, and matching children and spouses to names. For various reasons, however, some like to limit who can see contact and personal information. You can revise your privacy settings so this information is limited to administrators or the members of small groups or teams you're involved with. Of course, you can also make your contact information available to everyone with a login to your site.

## Procedure

- 1 Sign in to your office's Realm site.
- 2 Click your name in the upper-right corner, and select [Privacy](#).
- 3 Select your name or the name of a family member.
- 4 Select the privacy option you're comfortable with, or click [Custom Privacy](#) and select options for each field.
- 5 Click [Save](#).

# Understanding Privacy Settings

Learn what your privacy settings mean and how to keep your personal information protected.

| Privacy options                       | What this option means   |
|---------------------------------------|--|
| Anyone in the church                  | Everyone with a login, including office staff and congregants, can see your contact information and birthday. This option is not available to children.  |
| Leaders & groups/serving team members | Fellow group members and leaders can view your personal information. If you or a family member do not have a birth date on file, this option is unavailable. This setting also includes users with permission. |
| Leaders                               | Volunteers with leadership responsibilities can view your profile. If you or a family member do not have a birth date on file, this option is unavailable. This setting also includes users with permission.   |
| Users with permission only            | Administrators, office staff, and other people assigned by the office can view your profile and personal information.  |

## Tips for Using Realm Account Sign Up Requests Safely

Prevent scammers from requesting a Realm account.

If your church opts to set up Realm using Invite + Realm Account Sign Up Requests, anyone can request a Realm account. An admin will regularly need to review these requests in the [Overview Dashboard](#). Each request should be carefully reviewed by church staff.

As you know, the church is a popular playground for [scammers](#). Gaining access to a Realm site, would give a scammer the information and a trusted platform to launch some very successful [social engineering scams](#). A scammer works to be more believable, more legitimate, and poses as someone who wants to “help” their church. Allowing an impostor to have access to your church directory could disrupt your church community.

### Is it a Scam or a Legitimate Request?

If your church receives a request for a Realm account via email or through the Realm account request process, how do you know if the person is real? It's not always easy to determine.

**From:** Bill Bowden <[billbowdenchristchurch@gmail.com](mailto:billbowdenchristchurch@gmail.com)>

**Sent:** Thursday, March 30, 2023 8:17 AM

**Subject:** Set up realm account

Good day,

I'm a new member and I've been attending worship services, I was told to contact you to send an invitation to set up a [realm](#) account and Breeze account for online Giving.

Kind Regards,

Bill

### Ways to Verify

Bill's email and email address look a little suspicious, but is it possible that he could be visiting your church? It's not possible to know from that email, but there are a few ways you could handle this:



## Invitation Models and Best Practices

1. **Delete the email and see if he sends another email.**
  - This won't necessarily resolve anything.
  - If Bill is actually a phishing email, he may continue to email you. The same would be true for an actual person.
2. **Reply and tell him that he doesn't need an account to give online. Direct him to request an account on your church website.**
  - If he does this, your church will still need to determine how to verify if this is a legitimate request or a scam.
3. **Reply and say you're sorry you haven't met him yet.**
  - Ask him something about your church that can only be known by visiting - something that isn't posted online.
  - Or you could ask him to meet you at the next service. It would be unlikely that a "phish" would try to meet you in person.

## Security Takes All of Us

The security and privacy of your data is a shared responsibility.

Our relationship with our customers is built on trust. Protecting our customers' data is a responsibility we take very seriously. However, pastors and church leaders also bear responsibility in safekeeping data for members and the church.

People are increasingly sensitive about how their data is collected and used. The article can help answer some basic questions, but you'll want to invest time and resources into creating a plan for your employees and volunteer leadership to follow. Please visit [our legal section](#) regularly for information about our legal policies, FAQs, and advice for security tips and best practices. If you have any other questions, please feel free to email us at [risk@acst.com](mailto:risk@acst.com).

**🔗 TIP:** A subscription to MinistrySmart Pro Staff Pass provides access to several courses on the subject of protecting your office data. Log in to Realm. In the upper right corner, click the MinistrySmart Academy icon and search "Protecting Church Data" for a list of current courses.

Please visit our [Church Growth](#) blog for security and privacy related articles. In particular, check out these articles:

[Information Security for Staff and Volunteers](#),  
[Information Security for Congregants and Parishioners](#), or  
[Security for Your Computer and Systems](#).

## How ACST protects your Realm ChMS data

- Realm ChMS is hosted in [Amazon Web Services \("AWS"\)](#) US East 1 regional zone. The computer servers hosting Realm are implemented using AWS recommendations and industry best practice security configurations. All server configurations are extensively documented for compliance with the [Payment Card Industry Data Security Standard](#) .
- We encrypt and store all client data backups in redundant cloud storage locations for backup and disaster recovery with 24x7x365 access. Cloud storage data encryption uses AES 256 bit encryption.
- Each individual office's data is stored in a multi-tenant relational database. Internally, each office's data is stored in its own table. The table is indexed and accessed solely using unique ID's in the database. Any data needed is called by an algorithm call to either post data to or retrieve the data back from the database, ensuring integrity and segmentation. No data crossover is possible using this method.
- Only a limited number of authorized ACST employees located in the United States are allowed access to client data.

### How you can help protect your data

- Be sure you know you can see your personal information, and [update your privacy](#) settings accordingly.
- Administrators [should review new account registrations](#) daily when your office is using the open-invitation model.
- For the best experience, we recommend that you always update your browsers, whether you're using a computer, a tablet, or a mobile device. Using outdated browsers can introduce vulnerabilities and potentially allow malware or other threat actors into your system.
- Keep your operating system current and check the system requirements of the software vendors you use. If they allow operating systems that have experienced "end of life", they pose a threat to your system - even if your computers are up to date. For example, as of January 14, 2020, Microsoft stopped supporting Windows 7.
- Use strong, unique passwords and don't share passwords or logins with others.
- Use antivirus software and update it daily.