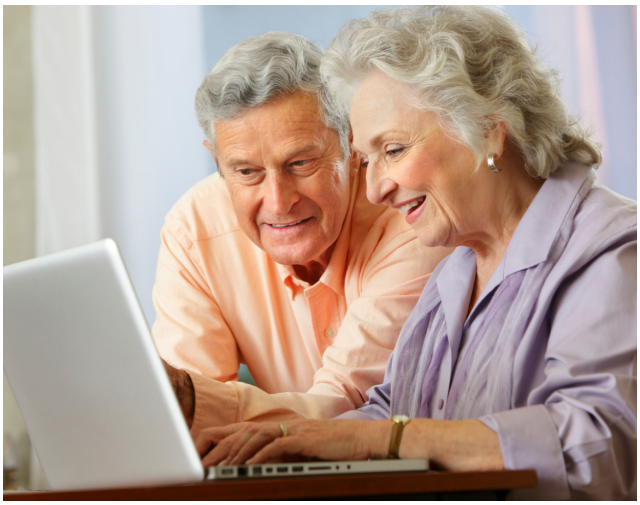
Tricks or Treats?:
Top Signs of Cyber Fraud

THE VILLAGE AT AUGSBURG
A National Lutheran Community



Want to hear something scary? When it comes to your online presence, there are monsters lurking in the shadows of your digital world! In this new age of technology, it has become nearly impossible to not have a presence and plenty of important, personal information online, and throughout the online world, just like in the real world, there are crimes, fraud and scams occurring every day. With new technologies and the ability to act anonymously, it can be difficult to tell who is real and who is trying to fool you into giving up personal information. Luckily, there are simple ways of telling the difference, but you must know the signs to look for.

Web browser warnings:

We are lucky to live in a time when our computers and security software have advanced enough to aid you in keeping your information, and the ways to access that information, safe. Web browser alerts are some of the most helpful ways to tell if something is a scam or fraud on the internet. With the security software, your internet browser is constantly searching for any signs that the site you are using is unreliable or unsafe. Your only job is to stay on the lookout for any alerts that might pop up from the browser's software. These alerts warn you if a site appears to be unsafe, so it is important to always pay close attention to your browser when alerts pop up and to read them thoroughly. This could be your web browser alerting you that the site you are on does not check out, or that you are at risk for potential scams or fraud attempts.

There's a prize or a problem:

Some of the most typical ways that hackers or scammers will influence your actions is through a prize or a problem. Prizes will often include some sort of quick pop-up advertisement stating that you are a "WINNER!" While this may seem like something to celebrate at first, it is important to take a closer look—you could pick up on some of the signs that this is in fact a fraud or scam attempt. These prizes will pop-up without warning sometimes with a lot of loud sound effects or bright colors, all meant to grab your attention as quickly as possible. The message might also say that you are a winner of a prize, but you do not remember entering any lottery or sweepstakes. These types of frauds might also ask you to send in money to cover taxes or administrative costs, or to require attending a meeting to collect that prize. Any of these signs could easily indicate that this is in fact a fraud or some sort of scam. Never click on any

links, give any money or share any financial information unless you remember entering said lottery and the sender is from a party or organization you are familiar with and have conversed with in the past.

Notifications of a problem can either appear as a pop-up or as an email or message of some sort. Often the message will be vague but have a clear sense of urgency and even aggression to them. This should be the first sign that tells you that this could be a fraud or some sort of scam. The message would most likely state that there is a problem of some sort, and in order to fix it, you need to click a link or give up personal information. That should be your second sign that this notification is a scam. Remember, you should never blindly give out your personal information over the phone or internet. If you are contacted and it looks like someone you do business with (such as your bank), it's always better to call the company directly, using their verified customer service number to see if they are trying to reach you.

Dependable domains and URL names:
Checking a domain or URL is a quick way to tell if something is cyber fraud or a scam. A link is one of the fastest and easiest ways that scammers and hackers can gain access and steal vital personal information. Learn how to spot the subtle differences in how a domain or URL is written out. Some examples include:

- Problems with spelling
- Inconsistent or incorrect punctuation
- Incorrect grammar or awkward phrasing

Spell check:
Often enough, those committing cyber fraud do not live in the U.S. or other English-speaking countries. As previously stated, you can thwart scammers by paying close attention to what they've written—keep a close eye out for errors or inconsistencies. It is also important to double check for grammar mistakes as well. Uncapitalized letters or misused punctuation can easily let you know that what you are reading likely did not come from an honest source.