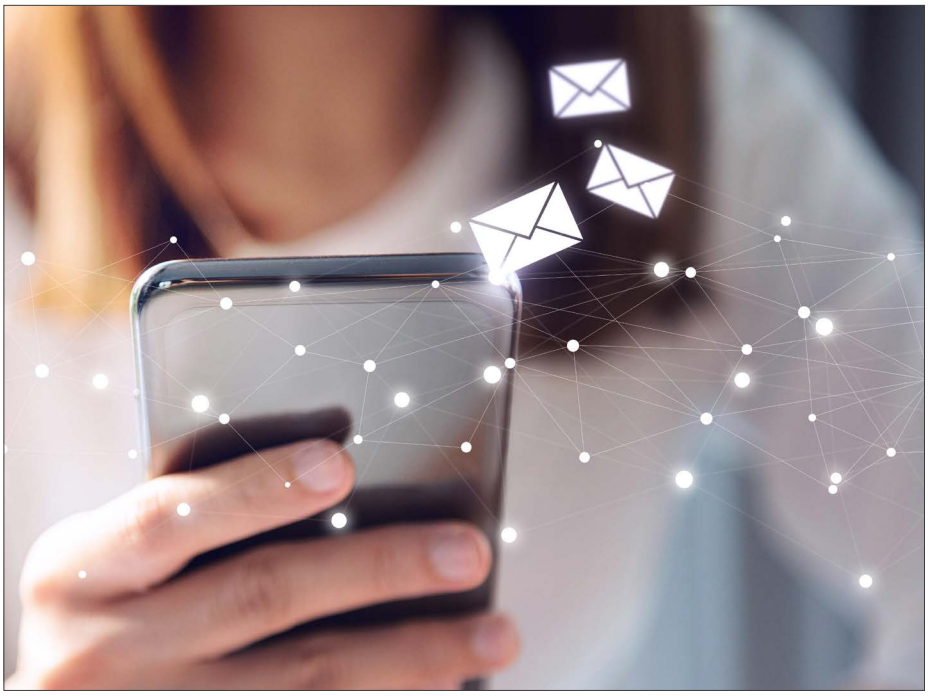
WFG National Title

SAFE Tipsheet

Email Security - Keeping it Safe

You can send and receive an email anytime, from anywhere - night or day - and never leave your comfy couch. It's fast, easy, and you can check it on the run. The point is, when you are reading, opening, and clicking on your email, you may not be at your most alert and may miss some clues you should be paying attention to.



Below are a few tips to start using whenever you open an email that could help you stay more secure in your hurried, distracted life.

Don't get spoofed! Check the "From" field in the email.

Make sure you know who it's coming from and that the address is correct. **MSmith@mycreditunion.com** and **MSmith@mycreditunion.account.com** are not the same! That second email is coming from whoever owns the "account.com" domain, not your "mycreditunion.com" bank's domain, and any response you send will be going to them as well - not to your bank.

Start with the ending. Check attachments for the file type.

File.doc (Word), **File.xls** (Excel), **File.tx**t (text) are safe files if they're coming from someone you know. But, ones ending in **.scr**, **.exe**, **.bat**, or **.com** are executable files, meaning they have code that executes or runs a program on your computer just by clicking on it.

You could also see a document name with multiple file types, like **File.doc.exe**, which may look safe, but whatever file type it ends in will be the real file type. Do NOT click on these or any file type you are not familiar with!

Practice hovering over all embedded links in messages.

Before you click that enticing link, be sure to hover your mouse over it to see where it's taking you because what you see may not be what you get. It's easy to create a link and hide the actual destination, so make hovering over every link in messages a habit. This can lead to better peace of mind and not to some nasty malware.

Overflowing inbox causing confusion and frustration?

Between spam, alerts, and other emails you previously subscribed to, it can be hard to find what's important or recognize any possible malicious email to avoid.

For spam, you should never reply to it, asking them to stop. It only verifies your email is active and will lead to more spam. Just delete the messages and block the senders.

For old newsletters and subscriptions no longer wanted, you can change your preferences or delete and block the sender as well. Don't use the "Unsubscribe" links as those could be compromised and can download a virus to your computer.