Princeton
Federal Credit Union
A Tradition of Financial Excellence

Safeguard Your Email

Email commonly transports malware also known as malicious software, like viruses, that can result in identity fraud or computer or device damage. In addition to viruses and worms that can be transmitted via email, phishing is another type of email fraud in which the perpetrator poses as a legitimate, trustworthy business in order to acquire personal and sensitive information, like passwords or financial data.

Tips to help you safeguard your email environment:

- Never include sensitive information in email. Forged email purporting to be from your financial institution or favorite online store is a popular trick used by criminals to extract personal information for fraud.
- Never open or respond to SPAM (unsolicited bulk email messages). Delete all SPAM without opening it. Responding to SPAM only confirms your email address to the spammer, which can actually intensify the problem.
- Never click on links within an email. It is safer to retype the web address than to click on it from within the body of the email.
- Don’t open attachments from strangers. If you do not know the sender or are not expecting the attachment, delete it.
- Don’t open attachments with odd filename extensions. Most computer files use filename extensions such as “.doc” for documents or “.jpg” for images. If a file has a double extension, like “heythere.doc.pif” it is highly likely that this is a dangerous file and should not be opened. In addition, do not open email attachments that have file endings of .exe, .pif, or .vbs. These are filename extensions for executable files and could cause damage to your computer if opened.
- Never give out your email address to unknown websites. If you don’t know the reputation of a website, don’t assume trust. Many websites sell email addresses or may be careless with your personal information.
- Don’t believe the hype. Many fraudulent emails contain urgent messages claiming your account will be closed if sensitive information is not provided immediately or that important security information needs to be updated online.
- Be aware of bad grammar, spelling and design. Fraudulent emails and websites often include typos and grammar errors as well as unprofessional design layout and quality.