An official website of the State of North Carolina How you know

State Government websites value user privacy. To learn more, view our full privacy policy (https://www.nc.gov/privacy).

Secure websites use HTTPS certificates. A lock icon or https:// means you've safely connected to the official website.

Avoiding Phishing Attacks

Phishing is a form of social engineering (https://www.us-cert.gov/ncas/tips/ST04-014). Cybercriminals use email. social media or malicious websites to pose as a trustworthy organization or person and solicit personal information. (Learn more about the different types of phishing.) (/resources/online-safety-privacy/tips-guidance/phishing/common-phishing-attacks)

For example, an attacker might send an email that seems to come from a reputable credit card company or financial institution. The attacker requests the user's account information and often suggests that there is a problem. When the user replies with the requested information, attackers can use it to access their accounts.

Phishing attacks might also appear to come from other organizations, such as charities, or even your company's IT support desk. Attackers often take advantage of current events and certain times of the year, such as:

- Holidays and other notable times of the year (e.g., tax season and election season)
- Natural disasters (e.g., hurricanes, tornadoes or earthquakes)
- Epidemics and health scares
- Economic concerns (e.g., IRS scams)

Simple Tips to Help You Protect Your Information & Devices

- **Think before you act.** Be wary of messages that implore you to act immediately, offer something that sounds too good to be true or ask for personal or financial information.
- **When in doubt, throw it out.** Cybercriminals often use links in emails and online posts to try to gain access to devices. If a message seems suspicious – even if you know the source – it is best to delete it or report it as spam.
- **Follow up.** Email and social media scams can be elaborate. If a message from a known sender seems out of the ordinary, check with the sender or poster using another method of communication.
- **Visit and download information only from trusted sources.** Carefully inspect websites you are unfamiliar with to be sure they are legitimate.
- **Use stronger authentication.** Enable multifactor authentication, when available, to help verify authorized access to online accounts.
- **Make passwords long and strong.** Combine capital and lowercase letters with numbers and symbols to create a more secure password.
- **Avoid clicking links in suspicious messages.** Instead, use a reputable search engine to get to the site or type the URL directly into your browser. If you choose to click a link, first verify its authenticity by hovering your cursor over the link to reveal the full address.
- **Do not reply to spam or click “unsubscribe” links in emails.** Doing so could confirm to the sender that your email address is valid or lead to malware being installed on your device. Instead, report the message as spam.
- **Connect only to trusted networks and use a reputable VPN when connecting to public wi-fi.** If you have a hotspot on your mobile device, use that instead. Unknown networks can be unsecure and can allow bad actors access to your devices.

- **Install and update anti-virus software.** Make sure your devices are equipped with regularly updated antivirus software, firewalls, email filters and anti-spyware.
- **Keep software up to date on your devices.** Reliable developers keep their products up to date to protect against online threats. Contact the service desk if you have difficulty installing updates.

Additional Tips to Reduce Spam

Following the above guidelines are not only good for security, but they can also help reduce annoying spam. Here are some more ways to help keep your inbox organized.

- **When possible, avoid publishing an email address on the web.** Spammers can harvest any email address posted online.
- **Check privacy policies.** Before submitting your email address (or any other personal information) online, read the site's privacy policy so you know how your information will be used.
- **Be aware of options selected by default.** When you must use your email for an online account or service, be sure any options to receive emails or mailing list subscriptions are deselected.
- **Consider using an alternate email account.** It can easily be deleted if spam becomes an issue or the email address is compromised. This can be used for newsletters, mailing lists and other registrations.

What to Do If You Think You Are a Victim

- **Report it.** If you believe you might have revealed sensitive information about your organization, report it to the appropriate people within the organization, including network administrators. They can be alert for any suspicious or unusual activity.
- **Watch for changes to your accounts.** If you believe your financial accounts may be compromised, contact your financial institution immediately and close any accounts that may have been compromised. Watch for any unexplainable charges to your account.
- **Change your passwords.** Immediately change any passwords you might have revealed. If you used the same password for multiple resources, make sure to change it for each account, and do not use that password in the future.
- **Watch for other signs of identity theft.** These signs could include (https://www.us-cert.gov/ncas/tips/ST05-019) but are not limited to:
  - Unusual or unexplainable charges on your bills
  - Phone calls or bills for accounts
  - Products or services that you do not have

- New, strange accounts appearing on your credit report
- Unexpected denial of your credit card