WaTech
Washington Technology Solutions
Washington's Consolidated Technology Services Agency

watech.wa.gov

Staying safe and healthy online during the coronavirus outbreak

Malicious actors are using the outbreak as an opportunity to launch online attacks. Read below for some tips to protect yourself.

As our work and home life changes in response to the coronavirus outbreak, many of us are spending more time online than usual. Threat actors are taking note and are seeking to benefit from this crisis. Now is a good opportunity to refresh yourself about basic cybersecurity steps you can take to stay safe online.

The state Office of Cybersecurity provides resources and best practices for staying safe online. During this outbreak, be especially mindful of the following common online scams:

- **Charity scams:** These types of scams target people who want to help by impersonating charities and other organizations in order to get personal information. Be wary of urgent messages requiring immediate action. Validate the email by calling the organization. Look up the phone number yourself. Do not call phone numbers provided in emails.
- **Domain spoofing of websites:** In this type of attack, bad actors will create a website that spoofs a trusted organization. Once you navigate to this spoofed page, you may be exposed to malware, credential theft, or fraud. To protect yourself**,** only go to trusted, known websites. Be wary of any website that immediately asks for your information or credentials. The state's official page for coronavirus related information is coronavirus.wa.gov, and other trusted sites are linked to from there.
- **Disinformation:** It is more important than ever during this time to ensure the information we rely on is accurate. To protect yourself**,** make sure the information you access comes from a primary and reputable source. Share information online with caution. Remember, relevant information shared by the state will be posted to coronavirus.wa.gov.
- **Phishing emails:** Threat actors are preying on the fear and uncertainty created by the pandemic to lure people into clicking on malicious links or download malware. Common tricks include claims for cures, face masks or other medical supplies, or vaccines. To protect yourself from becoming a victim, do not click on links or attachments in unsolicited emails.

This list is not exhaustive but serves as a reminder of core principles for navigating online safely. As we focus on staying safe and healthy during this time, be mindful of these tips to stay safe and healthy online as well.