PRESS RELEASE

UCOR

For Immediate Release

Contact:
Chris Caldwell
Christopher.Caldwell@orcc.doe.gov
(804) 658-8367

UCOR's top 10 tips for cybersecurity this season

Oak Ridge, Tenn., December 6, 2022 – During the holiday season, cybercriminals are trying extra hard to steal your information. UCOR's cybersecurity department is hard at work ensuring that every member of the UCOR team stays safe in the online world both at work and at home.

Following are 10 online security tips from our team that can help everyone keep their online information secure, especially during the holiday shopping season when those cybercriminals are more aggressive:

1) *Secure connections:* Be sure you have a secure connection before shopping. Look for "HTTPS" at the beginning of the URL address and a padlock icon in the address bar.
2) *Trusted WiFi:* Avoid using public WiFi for online shopping. However, if you have to use public WiFi, avoid entering sensitive information like your credit card number or login credentials that people could grab if they are eavesdropping on the public connection.
3) *Malware blockers:* Block your devices against malware by installing an extension on your web browser. This helps keep cybercriminals from building a profile on you.
4) *Vendor reputation:* Search for reviews of the vendor online to get an idea of the company's reputation and whether they are a reputable source.
5) *Phishing:* This is an online scam where criminals send emails or create websites that mimic legitimate businesses to steal your personal information. Because phishing campaigns can look like the real thing, be wary if you receive an unexpected email from a company where you don't have an account or if the website URL is slightly off. If you suspect you've been phished, **immediately** change your passwords to stronger ones and contact your bank or credit card company.
6) *Pay wisely.* Use a credit card or pre-paid debit card instead of a regular debit card linked to your bank account or, use a reliable, established third-party payment service, such as Google Pay, Apple Pay, or PayPal.
7) *Monitor accounts.* Check your online financial accounts regularly for suspicious spending. Also, take advantage of text and email alerting services offered by many banks and credit card companies.

8) *Never save payment information.* Saving your payment information on a website for convenience is risky. It leaves your information vulnerable during a data breach. Entering the information manually for each purchase takes longer, but it will help to keep your information safe.

9) *Use 2FA.* Two-factor authentication (2FA) gives you extra security and extra peace of mind. With 2FA, a code is generated and sent to your mobile phone for you to enter along with your password. It's an easy way to help protect your accounts from being hacked, even if your password has been stolen.

10) *Up-to-date software and antivirus.* Installing updated antivirus software will help protect against malware or other viruses. Also, be sure to maintain your computer's security by setting your computer to do automatic software updates so that you have the latest security patches.

UCOR is the DOE Oak Ridge Office of Environmental Management's lead environmental cleanup contractor. The company is a partnership between Amentum, Jacobs, and Honeywell. The company's 2,100+ workers are dedicated to safely reducing environmental risk on the Oak Ridge Reservation while helping DOE's Office of Science and the National Nuclear Security Administration continue their important missions. Learn more about the company at UCOR.com.

-end-

UCOR NR 2022-12