Jessica Hanna
202-828-7137
jessica.hanna@apci.org

FOR RELEASE ON RECEIPT

March 30, 2020

COVID-19: Insurers Provide Cybersecurity Tips for Working at Home

WASHINGTON D.C. — The coronavirus has forced more Americans to work from home or conduct other business online than ever before. The American Property Casualty Insurance Association (APCIA) reminds remote workers, businessowners, and online shoppers to be cyber aware and consider ways to protect against security breaches, identity theft, and other cybercrimes.

"As COVID-19 related phishing emails and other scams increase, it is a good idea to exercise greater caution to avoid becoming a victim," said David Sampson, APCIA's president and CEO. "Organizations that did not previously have widespread work from home programs, should ensure that employees have software installed on their computers that protects their company's data. Employees should avoid opening suspicious emails and links. While working remotely, it is also important to make sure that your wi-fi connection is secure or better yet, you're using your company's virtual private network (VPN)."

Following disasters and other emergencies such as the COVID-19 public health crisis, there is often an increase in fundraising scams. Before you click to donate or share personal and financial information like your Social Security number, date of birth or bank account number, investigate the charity to ensure it is a legitimate organization.

Online Safety Tips for Working at Home or Remotely:

1.) Use a secure network, such as your company's VPN. If you are using your personal home computer, make sure it has the same security protections as your work computer.

2.) Don't fall victim to an email phishing attack. These attacks will often try to trick you into sharing your personal information. Delete emails that look like spam or a scam.

3.) Closely scrutinize email links and be cautious opening attachments or downloading files from unknown sources. They could host malware that can infect your data or ransomware that shuts down your company's computer system.

4.) Always protect your passwords. When working remotely be sure that you don't leave passwords, PIN numbers, account numbers or other personal information exposed where someone could observe or steal them.

Online Safety Tips for Businesses:

1.) Make sure you have appropriate security measures in place to protect your customers' personal information.

2.) Make sure you have security software or firewalls to prevent someone from hacking into your site and taking the website down.

3.) Make sure you've tested e-commerce mechanisms from start to finish. Make sure everything is secure to protect both your business and the customer.

4.) Confirm with any third-party vendors, that they too have the proper security measures in place and are running a secure website.

Online Safety Tips for Shoppers:

1.) Make sure the website is legitimate, before you give out personal information make sure the site is secure.

2.) When sharing personal information online, never provide your social security number, passwords, financial information, or anything that could leave you vulnerable. It is also a good idea to check the site's privacy policy.

3.) Use a credit card when paying for something, rather than a debit card which has direct access to your bank accounts. Credit cards usually have a limit on how much you can spend. Be sure to review your statements, to see if there are any unauthorized charges. If there is a discrepancy, report it immediately.

The American Property Casualty Insurance Association (APCIA) is the primary national trade association for home, auto, and business insurers. APCIA promotes and protects the viability of private competition for the benefit of consumers and insurers, with a legacy dating back 150 years. APCIA members represent all sizes, structures, and regions—protecting families, communities, and businesses in the U.S. and across the globe.

###