

National Computer Security Day: Nov. 30 New Steps to Guard Against \$6 Trillion Cybercrime

3 Things Never to Do Online. 5 Key Steps to Stay Safe on the Web as Cybercrime Spikes

SALT LAKE CITY, UTAH, USA, November 24, 2020 /EINPresswire.com/ -- With National Computer Security Day on Nov. 30, 2020, Americans must be vigilant to fight the aggressive [cybercrime](#) world now that more Americans are working from home than ever before, according to an IT expert determined to keep computer users safe.



Fight Cybercrime Phishing Attacks

Cybercrime, which will exceed \$6 trillion annually by 2021, is up from \$3 trillion in 2015, according to [Cybersecurity Ventures](#).

“

Never use an auto login or free WIFI at hotels, airports or coffee shops, and never click a link you are not expecting in an email or text.”

Sarah Kimmel

“To stay safe online, I advise clients three things they should never do,” said Sarah Kimmel, CEO of Family Tech, which was established to help families manage the technology. “Never allow an auto login. Never use the hotel, airport or coffee shop’s free WIFI, and never click a link in an email or text you are not expecting.”

Today’s cybercriminals are much more efficient and are thriving financially in the dark web, which now has a lower barrier of entry than in years past.

“The dark web has commoditized attack tools, which gives attackers access to an excess of malicious capabilities, including ransomware as a service, botnets for rent, and malware as a service, to name a few,” said Kimmel, a Microsoft-certified IT manager.

Before COVID-19, roughly seven percent of Americans worked remotely. Today, more than 64

percent work from home.

“Because millions of U.S. workers and students were thrust into a [remote working learning](#) situation at home, they need to be aware of five key things to stay safe from cybercriminals,” she said. “First, set a lockout time, and use a password or biometrics to login. Change the default passwords on any devices or accounts to something unique.

“Next, use a VPN or your own mobile hotspot when on free public WIFI networks. Install and keep updated an antivirus program such as ESET. Educate yourself on various attack strategies like phishing, and back up your computer regularly.

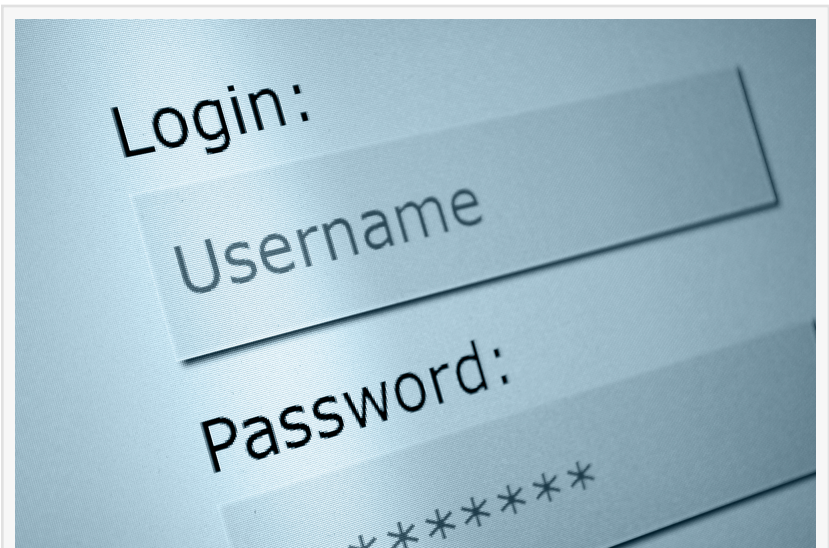
“Backups save time and data. While this doesn't seem entirely security-related, if your computer is compromised, restoring your computer from a recent backup is the best way to get your data back quickly.”

For more information on fighting cybercrime and staying safe on the Internet at home or at work, visit familytechzone.com.

A digital and IT expert, Kimmel is a Microsoft-certified IT manager who has supported over 100 small businesses since 2004. She also founded Family Tech LLC to help families understand and manage the technology in their home. Kimmel has regularly appeared as a family tech expert on TV and has consulted globally with tech companies, such as Microsoft, Dell, Samsung, Verizon and Lenovo. Visit familytechzone.com for more information.

###

Tim Brown
Candid Communications, LLC
+1 801-557-1466



Change passwords to something unique.



Use a VPN or your mobile hotspot when on free, public WIFI networks.

[email us here](#)

Visit us on social media:

[LinkedIn](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/531348428>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2020 IPD Group, Inc. All Right Reserved.