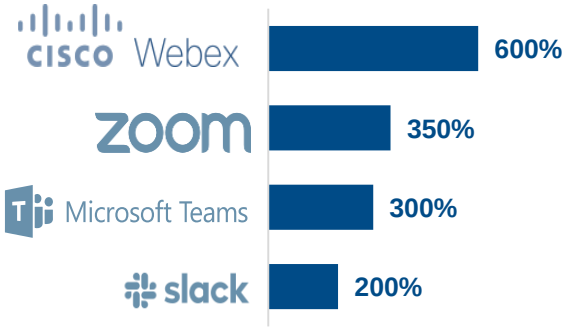
TIAA

Digital Security: Working from Home

TIAA Cybersecurity Program

Millions of employees are now working from home due to the COVID-19 pandemic. Before the outbreak, 27% of employees worked remotely. As of March, more than **60%** have started to work remotely[1], and with it, escalations of cyber threats have also gone up. Here are six cyber defense best practices for securing your work from home.

Remote work tool usage increase between January and April 2020[2]



What you can do to work from home securely

Practice good password hygiene

- Use two-factor authentication
- Never re-use credentials
- Follow corporate password requirements

Verify participants on conference calls and virtual meetings

Change default name and password on your router

It is best to change the network's SSID to something that does not disclose any personal information.

Use company-issued devices

Ensure devices, software and antivirus are patched and up to date.

Use VPN when connecting to remote wireless networks

Using VPN will encrypt your Internet communication and secure you from outside prying.

Stay Alert! Don't get phished

Phishing is the number one entry point for cyber-attacks. Learn how to spot phishing messages like a pro here►

Your security is our priority. For more information, please visit Security Center

Sources:

[1]Deloitte, Deloitte, Executive Cyber Briefing: Securing a Remote Workforce During COVID-19.

[2] McAfee, Working from Home in 2020: How Cloud Use Changed.