Digital Security: Working from home

Five tips to follow when working from home

Remote work has become increasingly common in the wake of the pandemic. While working from home has great benefits, a large outside-of-the-office workforce presents remote work security risks. Leverage these five tips to stay secure while working from home.

To work from home securely:

1. Use strong authentication to access your devices:
   a) Set up multi-factor authentication on all devices and accounts.
   b) Practice good password techniques. Password length is more important than complexity, although both are important.

2. Use of Wi-Fi:
   a) Avoid using public Wi-Fi. Data sent through public Wi-Fi can easily be intercepted.
   b) Change the default name and password on your router.

3. Use VPN when connecting and when connecting to your office network:
   a) A VPN (virtual private network) creates an encrypted “tunnel” for your network traffic to flow through and makes it harder for others to intercept your traffic.

4. Use company-issued devices:
   a) Ensure devices, software and anti-virus are patched and up-to-date.
   b) Do not use unapproved tools or store data outside of company resources.

5. Stay alert for phishing emails and phone calls.

At TIAA, customer data security is a top priority and we combine technology, people and processes to protect our customers and their personal information. We comply with both state and federal regulations and industry guidelines. For more information, please visit the Security Center.

©2022 Teachers Insurance and Annuity Association of America-College Retirement Equities Fund, 730 Third Avenue, New York, NY 10017