4 WAYS TO BOOST INFORMATION SECURITY AT HOME

The remote worker's guide to protecting data and staying aware of threats.

ORRIOS
The security and privacy experts.

USE ONE DEVICE FOR WORK ACTIVITY & FILES

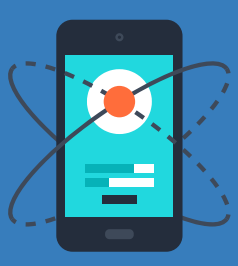
Multiple devices and access points create multiple vulnerability points for hackers. Dedicate one computer for work only and, if possible, use a Virtual Private Network (VPN) to access the company's systems and hosted files.

MAKE YOUR PASSWORDS HARDER TO CRACK

Creating memorable, secure passwords is easy. Using special characters to emulate birth month, middle name, birthday, and birth year - such as **01John02&%** - would take 121 millennia to hack.

AVOID SECURITY GAPS BY UPDATING YOUR SOFTWARE

Software updates help patch security flaws. So, make sure you're using the latest version of the operating systems, applications, and anti-virus software for your your computer and smartphone.



ADD AN EXTRA LAYER OF PROTECTION WITH 2FA

Two factor authentication (2FA) adds a stronger layer of security by requiring an extra piece of information to access systems in addition to your password. Google, LastPass, Microsoft, and others have 2FA options to fit your needs.

ONTRACK®

OnTrack® makes it easy to manage security requirements of remote workers, identify and document assets, manage and evaluate risk, execute risk mitigation plans, report to key stakeholders, and validate the effectiveness of information security and data privacy programs.
Learn more at ORRIOS.com.