Ostendio | Security Tips

ostendio.com

We are constantly using mobile devices yet often neglect putting in place proper security measures. Ensure that you have a screen lock or pin in place, update your data regularly, keep your OS updated and only install apps from trusted sources.

Would you hand over $100 if you were asked by a website? Treat your personal information like you would treat cash - protect it! Whenever you are asked for personal information check the source and always be skeptical.

Do you wait for months before installing computer updates? Try and update a minimum of once a week. Software and app updates contain important security updates which help to protect your device from threats.

Protect yourself on social networking sites by limiting the amount of personal information you share. Be wary of third party applications and strangers, and remember that the internet is a public forum. Only post information that you would be comfortable everyone seeing.

Talk to your IT team before installing plug-ins on your browser. When you install unauthorized software, from simple plug-ins to stand-alone programs, you may create a threat to your organization's security posture because the IT team will not include them in regular patches or fixes.

Protect sensitive data at all times. Use encryption when storing or transmitting sensitive data. Do not keep Social Security Numbers, credit card info, passport copies etc. on your workstation, laptop or mobile. Remove sensitive data files from devices when they are no longer needed.

Ensure that your identity is protected by having a firewall installed and enabled. Make sure that you keep your anti virus software updated, and always look for the "lock" on the browser's status bar.

Keep your portable devices safe. Always use a unique password. Disable Bluetooth functionality when it is not being used. Report lost devices to your carrier immediately and consistently review security settings to ensure that you have the appropriate protection you need.

Always be cautious of websites you visit. Stick with reputable online stores, news, and entertainment sites. Be sure to check the status bar at the bottom of your browser before clicking a link to make sure you are being directed to the intended site.

Copyright © 2020 Ostendio, inc. All rights reserved.

MyVCM

Ostendio | Security Tips

ostendio.com

Never walk away from your computer and leave the screen unlocked! Use an automatic screen lock on your device to ensure you are not open to intruders or malicious insider threats.

Think before you click! Cybercriminals are great marketers, and hide their viruses behind enticing titles, 'current news' and funny videos. Stop, and look at the link before you click.

Do you use your work device to access your personal email? This can expose your organization to additional risk. Just one infected personal email on your work computer can in turn infect the whole organization.

When you are surfing the internet, always use anti-virus and anti spyware software. Block pop-up windows and keep your operating system updated and patched. Never follow links provided by unknown sources.

Always monitor your accounts for suspicious activity. If you see something unfamiliar it may mean that you've been compromised. Bring your device to the IT team if you suspect that anything might be wrong.

Are you attending an out of office meeting or going on vacation? Before you leave, make sure your devices have been updated with the most recent patches, that your software is updated, and you have anti-virus installed.

Be careful about what you plug into your computer! USB's can contain malware. Opt for a high security USB stick with encryption and add password protection in case it gets lost or stolen. Do not borrow USB sticks, even from friends and colleagues.

Make passwords complex and secure. Everyone knows not to write them down but did you know that you shouldn't write down your user credentials as well? Ensure that both your password and user credentials are secure by not writing either of them down.

Create a unique password for your work login. Malware often steals login information from weaker systems such as online shopping sites. Reusing your work password can leave your organization open to compromise.

Connect With Us

@Ostendio

/company/ostendio

/ostendio

Copyright © 2020 Ostendio, inc. All rights reserved.

MyVCM