Ostendio

Security Tips

Do you walk away from your computer and leave the screen unlocked? Don't. You are ultimately responsible for everything done under your login. Put an automatic screen lock on your device to ensure that you don't leave yourself 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? If you do, you are exposing your organization to additional risk. Your work email has a number of systems in place to protect itself. If you open an infected personal email on your work computer, you can in turn infect the whole organization. Keep email use to personal devices.

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. Lastly, never visit untrusted websites or 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 your IT team if you suspect that anything might be wrong.

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

Be conscientious about what you plug into your computer. USB's can contain malware.

Passwords. We all know 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 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.

About Ostendio

Ostendio's MyVCM™ streamlines the way companies build, manage and demonstrate their information security framework. The MyVCM platform provides an enterprise view of an organization's cybersecurity program. MyVCM's unique bottom-up security approach provides a workflow solution which engages every employee and manages all aspects of security and

Ostendio, Inc.

1911 N Fort Myer Drive, Suite 100 | Arlington, VA, 22209
Phone: 1 877 668 5658 | Email: info@ostendio.com
www.ostendio.com

Ostendio

Security Tips

We are constantly using our 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 to 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 helps to protect your device from threats.

Facebook. Twitter. Snapchat. LinkedIn. 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. You can't take it back.

Do you have several plug-ins installed on your browser? Does your IT team know? If you install unauthorized software, from simple plug-ins to stand-alone programs, it can have a negative on your organization's security posture. IT may not include them in regular patches or fixes. Before you install software or a plug-in, let your IT team know.

Protect sensitive data at all times. When storing or transmitting sensitive data, always use encryption. Do not keep Social Security numbers, credit card details, passport copies etc. on your workstation, laptop or mobile device. Lastly, always securely remove sensitive data files 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 they're not being used. Report any lost devices to your carrier immediately and consistently review security settings to ensure that you have the appropriate protection you need.

Be cautious of websites you visit. Any website can be compromised, so 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.

About Ostendio

Ostendio's MyVCM™ streamlines the way companies build, manage and demonstrate their information security framework. The MyVCM platform provides an enterprise view of an organization's cybersecurity program. MyVCM's unique bottom-up security approach provides a workflow solution which engages every employee and manages all aspects of security and

Ostendio, Inc.

1911 N Fort Myer Drive, Suite 100 | Arlington, VA, 22209
Phone: 1 877 668 5658 | Email: info@ostendio.com
www.ostendio.com