POLICE DIGITAL SECURITY CENTRE ADVICE GUIDE

Tips to secure administrator settings

The ability to change the security and functionality of a device or program is known as an administrator. However, users that have administrator access as part of their standard user account could inadvertently cause a lot of damage if, for example, they are infected by a virus that deletes data.

No standard user account should have administrator access to your network.

Here are some tips to secure the administrative controls, both for your work network and at home:

Office Network	Home Network
Create a separate user account, ideally on an independent, clean device, to prevent cross contamination from everyday tasks.	Create a separate user account on a single home device, to prevent cross contamination from everyday tasks.
Restrict user access to reduce the impact of an attack should the network become compromised.	Adult only access to prevent children from accidentally changing settings that affect every device on the network.
Take the admin account offline to prevent compromise and unauthorised access.	Always log off the admin account when you have finished making changes.
Enforce strict policies: ■ No checking/sending/receiving emails to eliminate phishing attempts. ■ No browsing the internet to avoid malware infected websites and compromise of personal/financial/credential information. ■ No social media to avoid malicious adverts that spread malware or hijacks personal/financial/credential information. ■ No downloading/installing unnecessary apps to reduce the attack surface and entry points available to exploit through unpatched software. ■ No unnecessary activity that serves no purpose to the administrator role. With little activity, less can accidentally go wrong.	Avoid everyday tasks: ■ No checking/sending/receiving emails to eliminate phishing attempts. ■ No browsing the internet to avoid malware infected websites and compromise of personal/financial/credential information. ■ No social media to avoid malicious adverts that spread malware or hijacks personal/financial/credential information. ■ No downloading/installing unnecessary apps to reduce the attack surface and entry points available to exploit through unpatched software. ■ No unnecessary activity that serves no purpose to the administrator role. With little activity, less can accidentally go wrong.
Any administrative task carried out through the web browser must be whitelisted as a trusted source to avoid falling victim to spoofed websites looking to steal admin credentials.	Any administrative task carried out through the web browser must be whitelisted as a trusted source to avoid falling victim to spoofed websites looking to steal admin credentials.
Use a strong, unique password to lock the admin account at all times when not in use, to prevent unauthorised access.	Use a strong, unique password to lock the admin account at all times when not in use, to prevent unauthorised access, especially from children.
Enable 2 Factor Authentication where possible, in the event a password is compromised.	Enable 2 Factor Authentication where possible, in the event a password is compromised.

www.policedsc.com

PDSC
POLICE DIGITAL SECURITY CENTRE