Social Media & Cyber Security
ITS | Infrastructure Technology Solutions

Are you a business owner, manager or IT staff, and looking at the impact social media has on your network? Check-out best practice tips and options for social media security!

Social Media Policies:
Employers are more commonly introducing social media policies that address both the social media activity from the marketing department and official company accounts, and the social media policy and acceptable use guidelines for individual employees.

Security Risks:
Social Media, like many websites accessed from computers, tablets and phones, can contain spammy advertisements and links to nefarious sites. Many frantic browser hijack calls to our office begin with: *I was scrolling through facebook when suddenly...!* It is, unfortunately, quite easy to innocently scroll through a site, accidentally or purposefully click on something of interest, and find yourself in the midst of a **hijacked browser** (ctrl-alt-delete and task manager usually fixes this one) or **drive-by-download** (this is a virus or malware installed in the background when you visit an infected site).

Continue reading for tips on training users and setting up your network to minimize security risks.

Server-Side Browsing:
Some employees may access corporate apps and data via a remote desktop session, cloud-hosted desktop or other virtual desktop application. When using these technologies, users should NEVER perform browing or surfing functions on the same connection. Scrolling through facebook, searching for vacation sites or reading the news should be done on your local computer or personal device. Browsing from your server session puts corporate data and other users at risk.

BYOD
Companies that embrace a Bring-Your-Own-Device (BYOD) policy need to consider the same security scrutiny that a corporate asset faces. Does it have anti-virus/anti-malware software? Is corporate data stored on the machine? Can the machine be remotely wiped if lost, stolen or breached?

Guest Network Scheduling & Settings:
If you have business-class wireless hardware, you can setup seperate wirless networks (SSIDs) for work devices and guest/personal devices. This allows you to control the amount of time and/or bandwidth allocated to social media, allows you to keep users from accessing social media on corporate devices, and allows you to setup special permissions for marketing staff or other employees that need access to social media to perform job duties. Devices on the work network would have access to server shares, printers and other networked resources based on policies, and devices with guest access would only have access to internet.
Some offices take this a step further, and set the guest network on a timer, so visitors in your parking lot aren't able to camp outside and use your guest wifi after hours.