

RSACONFERENCE2014

FEBRUARY 24 - 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

The Dichotomy of the System Administrator

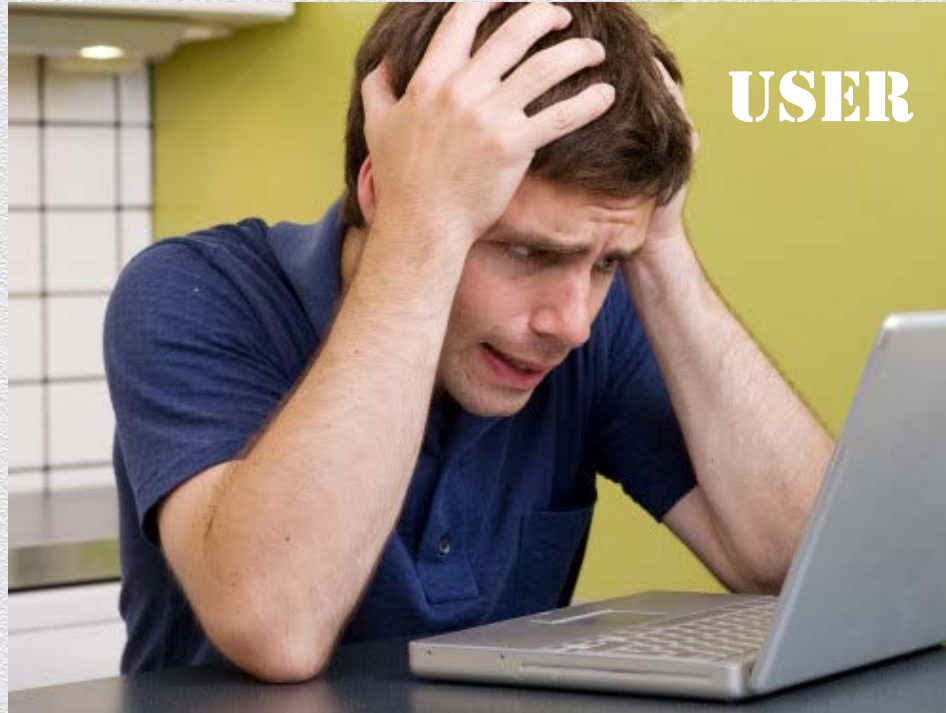
SESSION ID: GRC-F03A

Cliff Neve

Vice President
MAD Security/The Hacker Academy
@CommanderCliff



Throughout my career I have continually heard that this person is the problem.



But, I've found myself cleaning up *WAY* more messes from this person.



The Dichotomy of Administrator Usability vs. Security

- ◆ Administrators incented to help the user
 - ◆ All things being equal: usability has upper hand
 - ◆ Just make it work!!
- ◆ Senior level folks want easy
 - ◆ Often conflicts w/ security



Cyber Dumb that I have encountered:



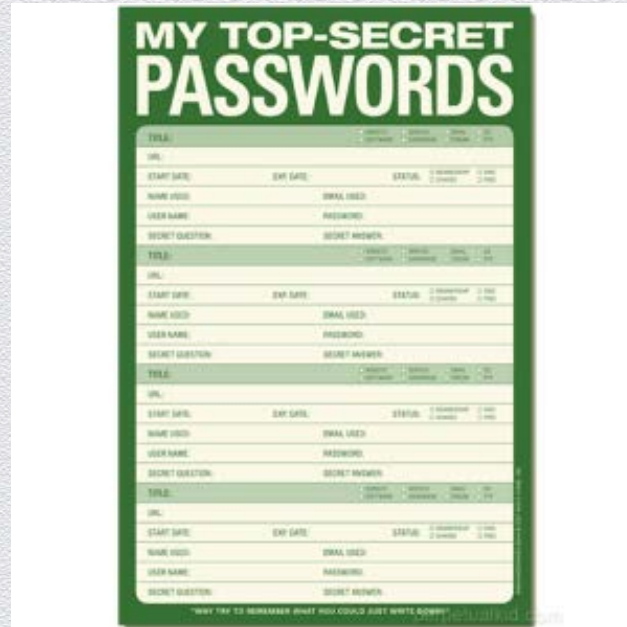
•



#RSAC

RSACONFERENCE2014

Keeping a spreadsheet of admin passwords for enterprise switches, routers, & apps..



and emailing to personal email.



Disabling security controls as 1st step of troubleshooting.



Downloading an unapproved 3rd party software that auto-installs driver updates.



Disabling 2-factor authentication to make it easier for certain “discerning” executive clients.



Not changing default passwords for devices including routers and VTCs.



#RSAC

RSACONFERENCE2014

Keeping a server from patch scanning for 3 years.



Solutions

- ◆ Executive commitment to security
- ◆ Centralize support and authority
 - ◆ Cuts down the drive-by overrides/impact of discerning senior customers
 - ◆ Need a quick waiver process
- ◆ Role based training
 - ◆ Separate and more advanced than user training
- ◆ Oral Boards and certifications
 - ◆ Significant emotional event...hammers home the importance

