Own IT. IT’s up to you.

Who wants to know?
There’s more than three billion people on the internet, and not all of them are who they say they are. Keep your friends list small, and never friend anyone you don’t know in real life.

The internet never forgets
With archive sites, screencaps and the quick spread of information on social media, the internet never forgets a mistake. You may dance like nobody’s watching, but post like everyone is.

Sharing is not caring
It’s tempting to share everything about your life, but what you share can be used by someone else. With that information, an attacker can impersonate you or break into your accounts on different sites.

Take it slow
Attackers will often goad people into making quick decisions, hoping to take advantage of your mistakes. Think fast, but type slow, and they can’t touch you.

© 2019 Infosec. All rights reserved.

UND Tech Support 701-777-2222 / UND IT Security Officer 701-777-5860
Own IT. IT's up to you.

A few good friends
The best way to keep yourself and your information safe is to limit your friends list and restrict what you post to your friends only.

<table>
<thead>
<tr>
<th>Friendbook</th>
<th>25 friends</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stacy Kingly</td>
<td></td>
</tr>
<tr>
<td>Georgie Red</td>
<td></td>
</tr>
<tr>
<td>Daryl Wentz</td>
<td></td>
</tr>
</tbody>
</table>

Bad share day
When you log into an account with a third-party app or service, information is being shared between that service and your account. Keep a lid on your data by using your individual login and not installing extensions.

Location unknown
If your location is known and being tracked by the phone in your pocket, then apps with that permission can access that data and follow you. Keep yourself hidden by turning off your location data.

Lockdown
A lock screen saves a lot of trouble in the long run. Even if your device is stolen, the attacker likely won't know your password. Enable encryption so that even if the lock screen is subverted, the data is still inaccessible.

Syncing ship
Disabling auto-sync forces someone who's stolen your account or device to enter your password, which will stop an attacker who doesn't know it.