

References

- <http://technet.microsoft.com/en-us/library/cc784090%28v=ws.10%29.aspx>
- <http://technet.microsoft.com/en-us/library/cc756109%28v=ws.10%29.aspx>
- <http://teens.webmd.com/features/teen-internet-safety-tips?page=2>
- <http://ia.unm.edu/pdf/outreach/Handouts/Internet%20Safety%20Guide%20for%20teens.pdf>
- <http://www.webmd.com/parenting/features/4-dangers-internet?page=3>

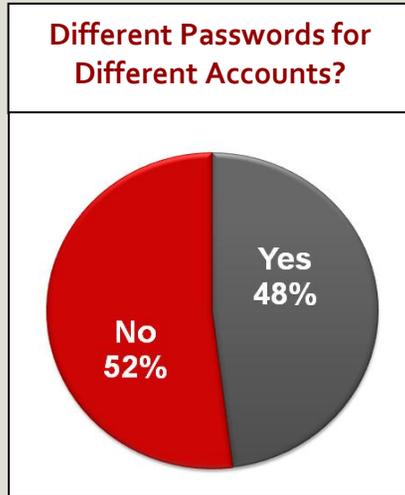


**Protecting Yourself from
Virtual Threats**

Password Best Practices

BASIC TIPS

- Always use strong passwords.
- If passwords must be written down on a piece of paper, store the paper in a secure place and destroy it when it is no longer needed.
- Never share passwords with anyone.
- Use different passwords for all user accounts.
- Change passwords immediately if they may have been compromised.
- Be careful about where passwords are saved on computers.



A STRONG PASSWORD

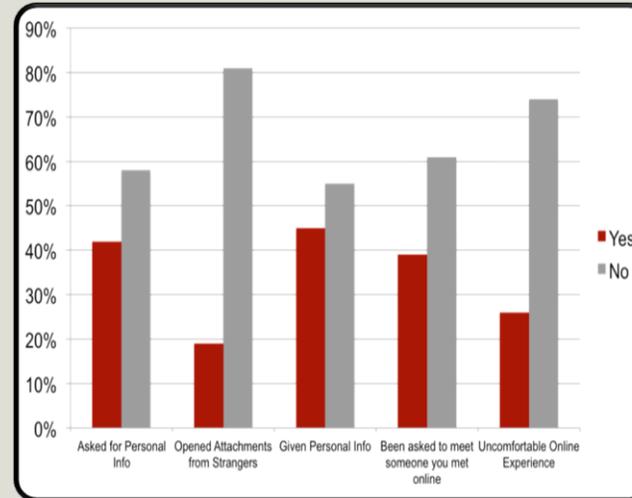
- Is at least seven characters long.
- Does not contain your user name, real name, or company name.
- Does not contain a complete dictionary word.
- Is significantly different from previous passwords.
- Contains characters from each of the following four groups:

Character Type	Examples
Uppercase letters	A, B, C ...
Lowercase letters	a, b, c ...
Numerals	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Keyboard Symbols	@ # \$ % ^ & * () +

A WEAK PASSWORD

- Is no password at all.
- Contains your user name, real name, or company name.
- Contains a complete dictionary word. For example, *Password* is a weak password.

Internet Safety



Facts

1 in 5 teenagers ages 10 to 17 have received unwanted sexual solicitation online

It may be difficult to distinguish who is a predator online

Since 2004, individuals ages 14 to 29 have the highest rate of identity theft

Universities, employers, and scholarships check your online presence and what they find can affect their decision.

Tips to Keep Yourself Safe Online

- Consider the pictures that you post online. Avoid putting pictures of yourself that are provocative or show you doing illegal activities, such as underage drinking, drugs, etc.
- Do not list personal information about yourself that would give an individual the pieces that they need to determine your identity or to locate you. This includes your phone number, address, interests, etc.
- Avoid listing your location on social media sites or allowing location services to be on your smart phone.
- Be cautious of who you communicate with online. Keep in mind that an individual may not be who they seem.
- Be aware of an individual who may be asking too much personal information or is beginning to ask you to meet in person. If a situation makes you feel uncomfortable, it is your conscious telling you that something is not right.
- Always report a situation that makes you feel uncomfortable or if an individual asks you to do something that you know is wrong to your parents and the local authorities. You can also call the ICAC investigators in NM at (505) 222-9000 or email them at www.NMCyberSafety.org.