bearaware

Computer Security Tips

Passcode Security

- **Only Use Strong Passcodes**
  A sufficiently strong passcode is *at least* 8 characters in length, contains a combination of upper-case letters, lower-case letters, numbers, and symbols, and is not a word, but a phrase or acronym.
- **Never Write Down Your Passcodes**
  If you write your passcode someone can find it. Create secure passcodes that are also easy for you to remember.
- **Do Not Share Your Passcodes**
  Once you give your passcode to a family member or friend you no longer control the security of your data and personal information.

Laptop Security

- **Treat Your Laptop like Cash**
  Just as you would not leave money laying around in plain view, never leave your laptop unaccompanied in a public place - even for "just a minute" - or in a locked car.
- **Do Not Carry A Laptop Bag**
  Laptop bags advertise that you have a laptop. Consider using a padded briefcase or a backpack instead.
- **Consider Using Additional Security**
  Cable locks (with and without alarms) are widely available for laptops and can act as a deterrent to theives.
- **Be Aware When You Travel**
  Monitor your laptop carefully as it moves through airport security screening checkpoints, and be sure to carry it on the airplane.

Internet Security

- **Use Anti-Virus Software**
  Anti-virus software (like Symantec) monitors your system for suspicious activity and regularly updates itself against new threats.
- **Phishing E-Mails**
  If you receive an e-mail from a bank, eBay, PayPal, or another company, do not use the links included. Always log directly into the company's web site.
- **Spearing E-Mails**
  If you receive an e-mail from Baylor requesting your login information, do not click the links or reply to the message. Remember that Baylor will NEVER ask for your password in an e-mail, on the phone, or in person.

If you believe that your computer or your personal information has been compromised, or if your laptop is stolen, call Baylor Police at x2222.

http://www.baylor.edu/bearaware/

bearaware

Computer Security Reference Card

Passcode Security

- **Only Use Strong Passcodes**
  A sufficiently strong passcode is *at least* 8 characters in length, contains a combination of upper-case letters, lower-case letters, numbers, and symbols, and is not a word, but a phrase or acronym.
- **Never Write Down Your Passcodes**
  If you write your passcode someone can find it. Create secure passcodes that are also easy for you to remember.
- **Do Not Share Your Passcodes**
  Once you give your passcode to a family member or friend you no longer control the security of your data and personal information.

Laptop Security

- **Treat Your Laptop like Cash**
  Just as you would not leave money laying around in plain view, never leave your laptop unaccompanied in a public place - even for "just a minute" - or in a locked car.
- **Do Not Carry A Laptop Bag**
  Laptop bags advertise that you have a laptop. Consider using a padded briefcase or a backpack instead.
- **Consider Using Additional Security**
  Cable locks (with and without alarms) are widely available for laptops and can act as a deterrent to theives.
- **Be Aware When You Travel**
  Monitor your laptop carefully as it moves through airport security screening checkpoints, and be sure to carry it on the airplane.

Internet Security

- **Use Anti-Virus and Anti-Spyware Software**
  Anti-virus software (like Symantec Norton) monitors your system for suspicious activity and regularly updates itself against new threats. Anti-Spyware software (like Ad-Aware or Spybot) scans your system for common adware/spyware packages on your computer. Use these in tandem to protect you and your computer.
- **Think Before You Click!**
  If you receive an e-mail from a bank, eBay, PayPal, or another company, do not use the links included. Always log directly into the company's web site.

If you believe that your computer or your personal information has been compromised, or if your laptop is stolen, call Baylor Police at x2222.

http://www.baylor.edu/bearaware/

bearaware

Social Networking Security Tips

General Concerns

Choose Your Friends Wisely
Do not accept friend requests from unknown individuals, who are often phishers, spammers or, worse, identity thieves.

Manage the Personal Information You Share
Some social networks make all of your information public by default or share your information with your friend's friends. Learn how to use the access controls on your social network and check them regularly.

Check Your Tags
Be sure that you know what you are being "tagged" to and what controls are available to help you remove "tags" that you do not want associated with you

Application Concerns

Choose Applications Carefully
Use the same care installing social networking applications that you do with applications on your computer. Rogue applications exist on social networks that will attempt to steal your information.

Manage Information Access
Always consider whether you want the application or its creator to have access to the information in your social network before installing.

Never Share Passwords
Do not share your social networking passwords through applications or websites that you are not confident will protect the information.

Location Awareness Concerns

Limit Access to Your Location Information
Sharing specific location information reveals both where you are and where you aren't. Share it only with your closest friends and family, if at all

Be Aware of Embedded Location Tags
Some smartphones tag location information in photos and, when uploaded, this data becomes available. Disable these tagging features unless they are desired.

Work-Related Concerns

Be Aware of What You Share About Yourself
Many employers check social networks before interviewing or hiring potential employees, so be sure you portray yourself carefully.

Be Aware of What You Share About Your Work
Talking about your work environment, work-related information, an anonymous co-worker or a client with context may put your job, and your company, at risk.

Reserve Social Networking for Personal Time
Think before accessing your social network from work. Some employers monitor and regulate the use of company networks for social networking.

bearaware

Social Networking Security Tips

General Concerns

Choose Your Friends Wisely
Do not accept friend requests from unknown individuals, who are often phishers, spammers or, worse, identity thieves.

Manage the Personal Information You Share
Some social networks make all of your information public by default or share your information with your friend's friends. Learn how to use the access controls on your social network and check them regularly.

Check Your Tags
Be sure that you know what you are being "tagged" to and what controls are available to help you remove "tags" that you do not want associated with you

Application Concerns

Choose Applications Carefully
Use the same care installing social networking applications that you do with applications on your computer. Rogue applications exist on social networks that will attempt to steal your information.

Manage Information Access
Always consider whether you want the application or its creator to have access to the information in your social network before installing.

Never Share Passwords
Do not share your social networking passwords through applications or websites that you are not confident will protect the information.

Location Awareness Concerns

Limit Access to Your Location Information
Sharing specific location information reveals both where you are and where you aren't. Share it only with your closest friends and family, if at all

Be Aware of Embedded Location Tags
Some smartphones tag location information in photos and, when uploaded, this data becomes available. Disable these tagging features unless they are desired.

Work-Related Concerns

Be Aware of What You Share About Yourself
Many employers check social networks before interviewing or hiring potential employees, so be sure you portray yourself carefully.

Be Aware of What You Share About Your Work
Talking about your work environment, work-related information, an anonymous co-worker or a client with context may put your job, and your company, at risk.

Reserve Social Networking for Personal Time
Think before accessing your social network from work. Some employers monitor and regulate the use of company networks for social networking.