BUREAU OF EDUCATIONAL AND CULTURAL AFFAIRS

Your Safety and Security Online: Safety Tips

The U.S. Department of State's Bureau of Educational and Cultural Affairs takes your online safety and security very seriously. As you use social networks, e-mail, and the Internet, please consider the following **Safety Tips:**

1. Never broadcast private contact information. Never list your e-mail address or phone number in any public space, such as your profile page, a blog, forums, or photo caption.

2. If you are a member of a social network, pay close attention to your privacy settings, which allow you to choose how much personal information you reveal and to whom.

3. Carefully consider what you publish on social networks. Before you post photos, videos, or text, ask yourself if it would embarrass you if your family or employer saw them.

4. Before you add a widget (an application that can be shared with others electronically) to your profile, think about whether you want the creators of the widget to be able to access your profile page and information about your activity on the social network. Keep in mind that the social network generally has no control over these widgets, so exercise discretion when using these tools.

5. Report any abuses of a website's Terms of Use to the website's administrators. Any reputable website or social network will have a way for you to report abuses.

6. E-mail can be used to spread malicious software or obtain your personal information in order to commit fraud.

To protect yourself and the computers that you use, follow the guidelines below:

- Be suspicious of unsolicited e-mail messages or phone calls from individuals asking for personal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with that organization.

- Never provide personal or financial information (credit card numbers, PIN numbers, identification numbers) in response to e-mails or telephone calls that you did not initiate.

- Do not send personal or financial information over the Internet before checking the website's security. (Secure website addresses begin with "https://")

- Pay attention to the address of a website, located at the top of the screen. Malicious web sites may look identical to a legitimate site, but the address may use a variation in spelling or a different domain (e.g., ".com" vs. ".net").

- Protect your computer and other computers that you use by scanning all removable media, such as a flash drive, CD, or DVD, for viruses before opening files that are contained on the media and by scanning all attachments that you receive via e-mail prior to opening them.

- Do not accept or open executable files (indicated by a file name ending in ".exe") that you receive via e-mail. Such files can be dangerous.