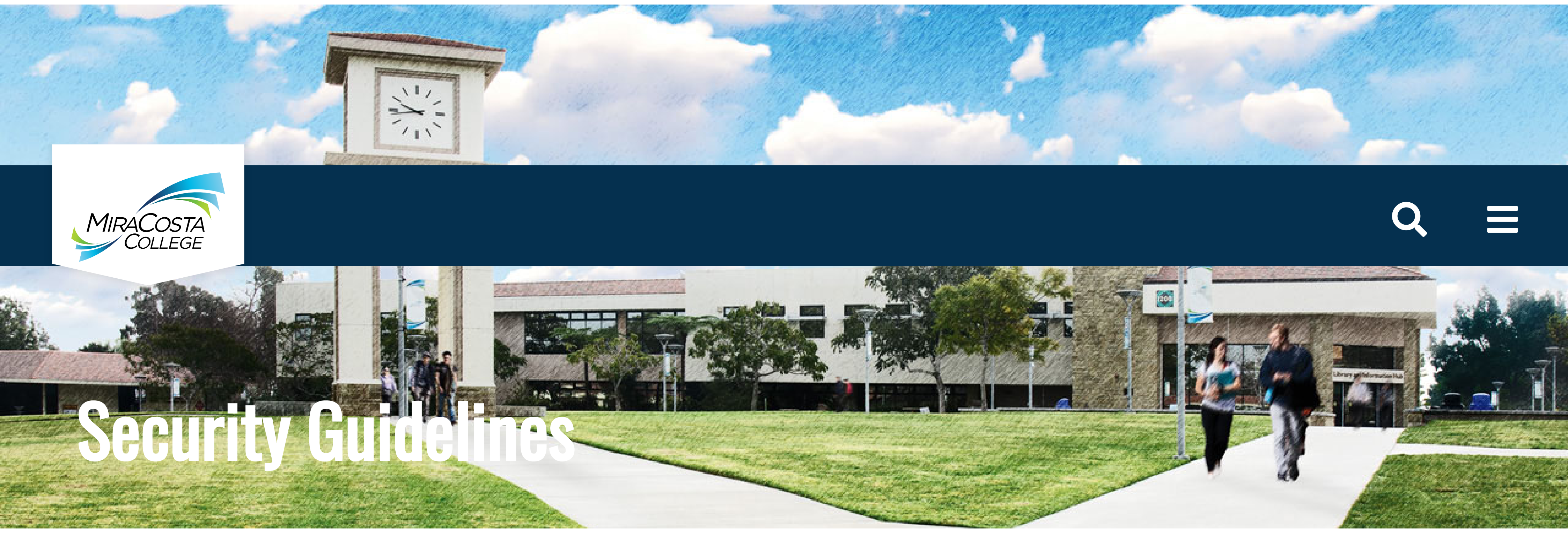
RETURN TO CAMPUS: CLICK TO LEARN MORE



Security Guidelines

HOME / FACULTY STAFF / ACADEMIC INFORMATION SERVICES / INFRASTRUCTURE SYSTEMS / SECURITY GUIDELINES

Select Language

IN THIS SECTION

Computer security is becoming more important all the time. Global spending cybersecurity is over $100 billion annually. In recent times it has become commonplace for public agencies to experience devastating computer breaches.

These are basic guidelines that can be implemented by you with as little difficulty and expense as possible. These measures are listed in order of importance.

- Phishing
- Backups
- 2 Factor Authentication
- Patches
- Malware
- Passwords
- Email Attachments
- Encryption
- Firewalls
- Other Precautions
- Security Links

Understand Phishing

Phishing

Phish is spam email that is “fishing” for information such as your logon name and password.
Phishing currently is THE most common entry point for a security incident.

- Phish may come from an [EXTERNAL] source when an internal source would be expected.
- Phish might entice you to take some sort of action, such as reset your password, open a file, or view a web page.
- Phish may appear to come from people and organizations you trust.
- Phish will most often include a link for you to click. Usually, the link takes you to a form where it would like you to enter your name and password.

Spear Phishing

"Spear phishing" is targeted at a specific individual or small group of individuals.

- Targeted Phishing sites may have a login page which looks identical to existing to the sites actual login page.

- Targeted Phishing sites may harvest your credentials on a fake login page, and then seamlessly log you into the actual site.

If you suspect phishing

- Navigate to the website using a bookmark or search, rather than clicking an embedded link
- If you are unsure whether or not the message is legitimate, either delete the message or open a helpdesk ticket.

- If you fall prey to phish by giving up your name and password, it is important you change your password right away. Please call our helpdesk at 760-795-6850.

More Information

- Avoiding Social Engineering and Phishing Attacks
- 8 Things You Should Understand About Phishing
- Anti-Phishing Working Group

Backups

Having backups is an effective countermeasure for many possible issues, including:

- Ransomware
- catastrophic system error
- accidental deletion

Any data that you consider valuable should have a reasonably up-to-date copy (also known as a backup) stored somewhere other than your computer's hard drive. Copying your important files to a USB drive or a cloud storage provider such as Google Drive or Office 365 would be good enough for most home computers. **NOTE:** while the backup drive is connected it is vulnerable to many of the same issues.

Two Factor Authentication

Username and a password authentication is no longer considered adequate security, especially for high value accounts such as online banking, shopping, or email.
To effectively authenticate a person additional factors beyond a password are required. Two Factor Authentication (2FA) or Multi Factor Authentication (MFA) uses something you know (your password) and something you have (your smart phone, a hardware token) or something you are (your fingerprint, etc.) to make it more difficult to take over your accounts. Staff and Faculty Enable Multi Factor Authentication

Patches

A patch is software that fixes a bug in a program. Having your system properly patched one of the most effective things you can do to increase the security of your computer. Patches are released frequently and should be kept current.

Operating System Patches

For most computers, you can select Windows Update from the Start Menu or Settings Menu. Modern operating system have an automatic update function. Make sure it is enabled. Consult your operating system vendor for details.

Application Patches

Browser, email, and virus protection applications publish patches on a regular basis. Many of these have an automatic update function. Contact the software vendor for details. Updating Java and Flash are critical as these are the most often exploited apps. Update items in the Apple App store, Google Play store, and other vendor application repositories.

Malware Protection

Malware protection software attempts to keep malicious code from running on your computer. Having malware protection software installed and updated is important to protect your personal computer.

Passwords

You should never share your password with anyone else. It is against our acceptable use policy, and a bad idea.
Every site should have a unique password.

General Considerations

- Any default passwords or passwords received via email should be changed.
- Consider using Two Factor Authentication.
- Consider using a password manager.

Good Passwords

- Good passwords are long -- the longer the better.
- Good passwords contain upper and lower case letters, numbers, and symbols.
- Good Password are something you can remember

Bad Passwords

- Bad passwords are used on multiple accounts.
- Bad passwords are words found in dictionaries: password
- Bad passwords are alphabetical, numerical, or keyboard sequences: abcdef, 123456, querty
- Bad passwords are easily guessable or learnable information: pet's name, etc.

Email Attachments

Unless you are expecting an attachment, don't open it. Even if the email is seemingly from a trusted source such as a bank or a good friend. As a simple check, you can send the person a message to confirm if they really sent you the email with an attachment(s).

Encryption

Encryption makes it more difficult for unauthorized persons to read the data you send and receive from or store on your computer. Make sure your browser has the closed padlock in the address bar before entering a password or other sensitive data, shopping, or banking online. If you have files with sensitive data, consider encrypting the files. Learn how to send encrypted email.

Firewalls

A firewall is a device or program that attempts to prevent access to a computer system or network from outside of that system or network. It is strongly recommended that you have some sort of software or hardware firewall installed. Most modern operating systems and home networking devices have firewall software installed. Make sure it is enabled and configured properly.

Other Precautions

More Things You Can Do To Improve Your Security

Consider Email Public and Instant Messaging. Any email sent to or received from an external (non-MiraCosta) address is transmitted in clear text and could potentially be intercepted in transit. These emails have [EXTERNAL] in the subject.

Wireless Networks. Unless you are using WPA2 and the latest firmware on your access point(s), wireless networks are difficult to properly secure. Unless you're sure you've properly secured your wireless network. limit your exposure by leaving your wireless router off when not in use and consider anything transmitted without end to end encryption public. Make sure to change the default password to you wireless access point and disable management over WiFi.

Review you Web Browser's security and privacy settings.

Turn Off Unused Services. Any operating system services or other programs that aren't needed should not be running. This not only increases your risk but may impact performance as well. NOTE: Use caution when turning off services. Some services are required for your computer to operate properly.

Use a Surge Protector or UPS. You can avoid damage to your computer equipment by plugging it in to a surge protector. A UPS (Uninterruptible Power Supply) will use batteries to keep your computer running during a short power outage. The cost of a UPS isn't normally worthwhile for a home computer, but it is an option to consider.