CAMPUSGUARD®

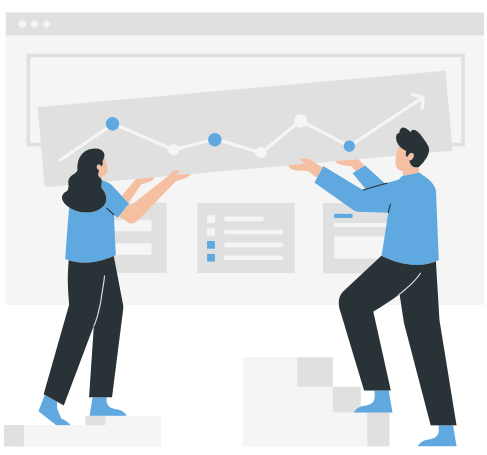
Information Security Best Practices

What Is Information Security?

Information security is the protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction, in order to provide confidentiality, integrity, and availability

Confidentiality: Information is only available to authorized individuals, entities, or processes

Data integrity: Ensuring that the data is as expected and hasn't been modified without appropriate authorization



Availability: Information must be available when it is needed, and information security provides the processes to support that requirement

All users are responsible for information security!

CAMPUSGUARD®

Personally Identifiable Information

Personally identifiable information (PII) is any data that could potentially identify a specific individual

- Names and addresses
- Social security numbers
- Account numbers
- Dates of birth
- Drivers' license or passport numbers
- Digital signatures
- Biometric data and fingerprints

Personally identifiable information can be used by criminals to commit fraud, so should be kept confidential and protected by adequate security controls

CAMPUSGUARD®

Common Security Tools

(and why they are so important!)

Vulnerability Scans: Look for vulnerabilities, misconfigurations, and outdated software so any areas of concern can be remediated

Software updates/patches: Upgrade a piece of software to the latest version, improve an application's stability, or fix a bug or security hole within the program

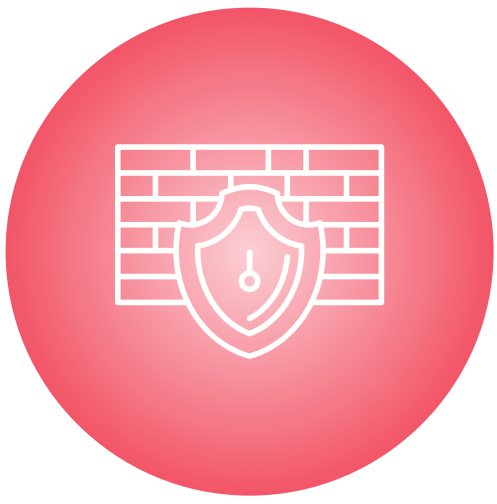
Spam blockers: Block junk, malicious, and phishing email messages

Anti-virus and anti-spyware applications: Scan files, and detect and remove malicious software

Virtual Private Network (or VPN): Creates a secure network connection between a remote device and a host network

Common Security Tools (continued)

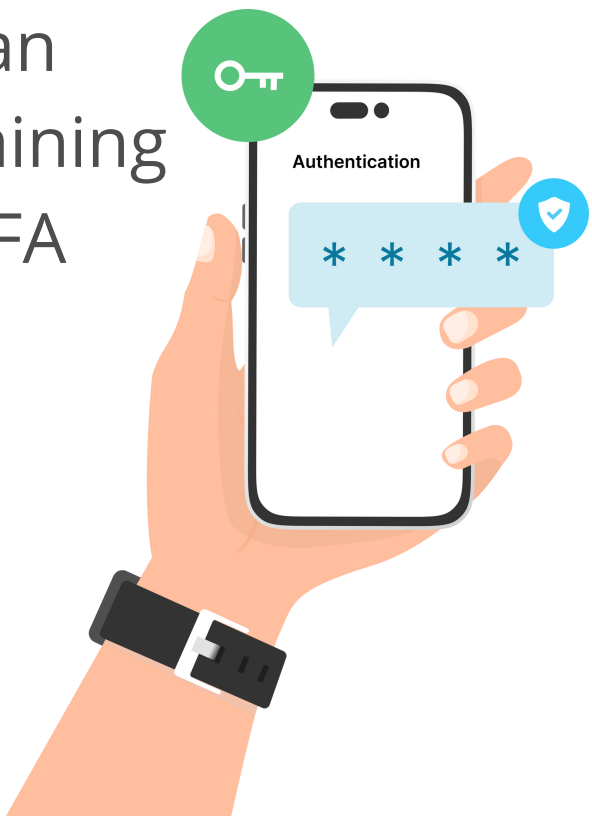
Firewalls: Restrict or allow different types of information to pass in and out of networks, servers, or PCs



Intrusion Prevention Systems (or IPS) and Intrusion Detection Systems (or IDS): Monitors networks for indicators of malicious activities, and notifies your IT team when something suspicious has been detected

Multi-factor authentication (MFA):

MFA adds another layer of security to the authentication process which prevents anyone other than an authorized individual from gaining access to a secure system. MFA requires a combination of at least two different types of authentication:



- Something you know – username and password
- Something you have – a USB hardware token, or mobile device, phone, etc., that allows you to confirm your identity
- Something you are – biometrics like a fingerprint, retinal scan, or facial recognition

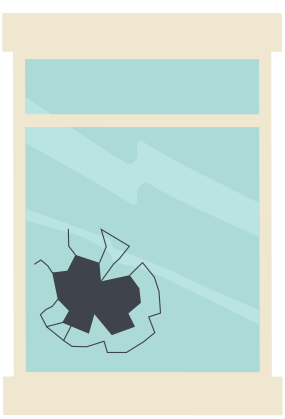
CAMPUSGUARD®

Physical Security Reminders

Best practices and basic steps to physically securing your environment include:

Secure access to keys, badges, access cards, and uniforms

When you enter a secure facility, do not hold the door open even if you know the person. Don't allow the person behind you to enter without his or her own key or badge



Report all broken doors, windows, and locks to facilities management

Monitor and report suspicious activities or concerning behaviors immediately

Physical Security Reminders (continued)

Maintain an accurate inventory of critical devices, hardware, and software

Place all media containing confidential information in secured locations

Limit access to sensitive information

Don’t leave sensitive documents unattended

Lock your door when you step away

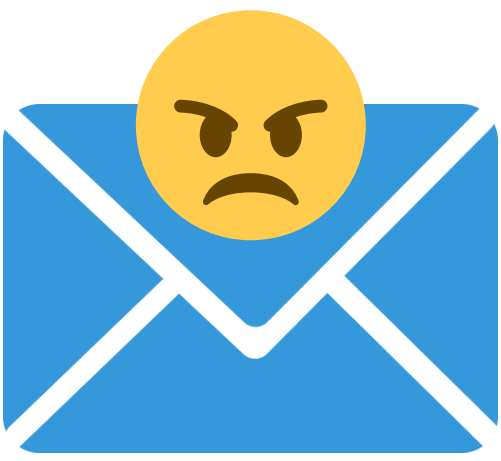
CAMPUSGUARD®

Email Best Practices

Before you hit SEND on an email message, you should always confirm the following:

Are the name and email address in the TO field correct? Many email clients will automatically fill in a name when you begin typing. Double check that you did not end up with the wrong recipient.

Is the content appropriate?



Does your tone convey the message well or could it be misread and lead to a misunderstanding?

Consider the attachments—have you attached the correct document?

Email Best Practices (continued)

Are you sharing sensitive information that should not be emailed (i.e. sensitive health information, student records, etc.)?

Is the recipient expecting an attachment or will they delete your message thinking it is spam?

Are you taking into account any potential consequences that might arise if your email was shared or forwarded to others?

Do not include language or statements that are not accurate and professional.

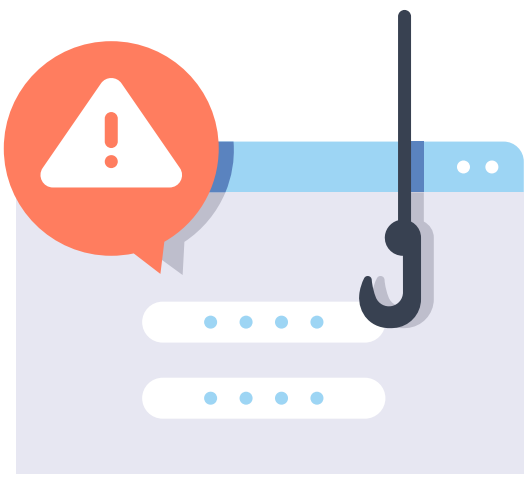
Ensure that the email complies with your organization's acceptable usage policies.

CAMPUSGUARD®

Phishing Warning Signs

There are several warning signs that can indicate an email is a phishing attempt.

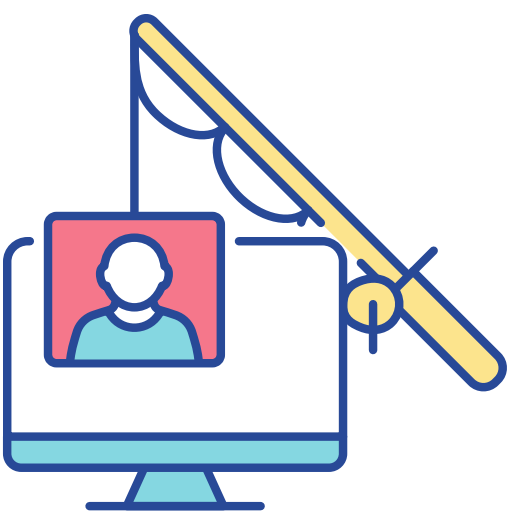
Here's what to look out for:



Emails requesting login credentials, payment information, or other sensitive information should always be treated with caution.

Organizations should not request this information via email.

It is written with a sense of urgency so that you will respond immediately without questioning if the request is valid.



The “from” address is spoofed so that the email appears to come from a known or trusted source.

Phishing Warning Signs (continued)

The "to:" field is blank or the email is not addressed to you specifically.

Spelling and grammar errors exist.

Links to unfamiliar or strange websites are included, but may be disguised as genuine links.

If an email with an attached file is received from an unfamiliar sender, or if you did not request or expect to receive a file, any attachments should be opened with caution.

CAMPUSGUARD®

You've Been Hacked

If you believe your email account has been compromised, you should take the following steps:

Report the incident to the IT help desk and follow any recommendations they provide for your situation.

Refer to your organization's incident response plan for specific guidelines.

If you have used the same password on other websites, immediately change the passwords on those sites and replace each with a unique and different password.

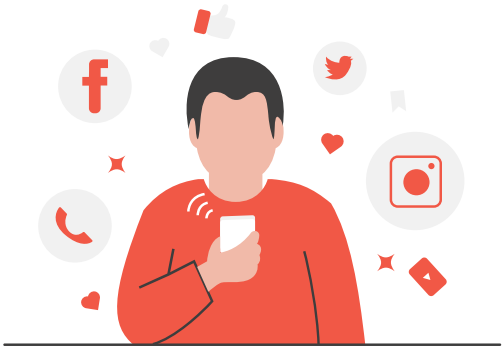
Review all of your email folders for messages that may have contained sensitive information.

Be on the lookout for suspicious account activities over the next several months.

CAMPUSGUARD®

Be Safe When Social Networking

Limit the amount of personal information you post

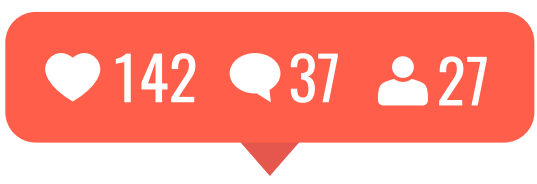


Only post information you are comfortable with absolutely ANYONE seeing

Note: Posting a picture of yourself at the airport awaiting your flight gives criminals the inside track to your location (and your empty house)

Review and take advantage of the social network's privacy settings

Be skeptical of requests from new followers, and consider declining those that you don't know



Don't believe everything you read online

CAMPUSGUARD®

Preventing SPAM

Be cautious about posting your email address on websites that allow anyone access to that information.

Review privacy policies of websites before sharing your email address on them.

Don’t reply to spam—not even to request to be removed from the mailing list.

Don’t send read receipts.

Don’t register on websites offering prizes or contests that seem just too good to be true.