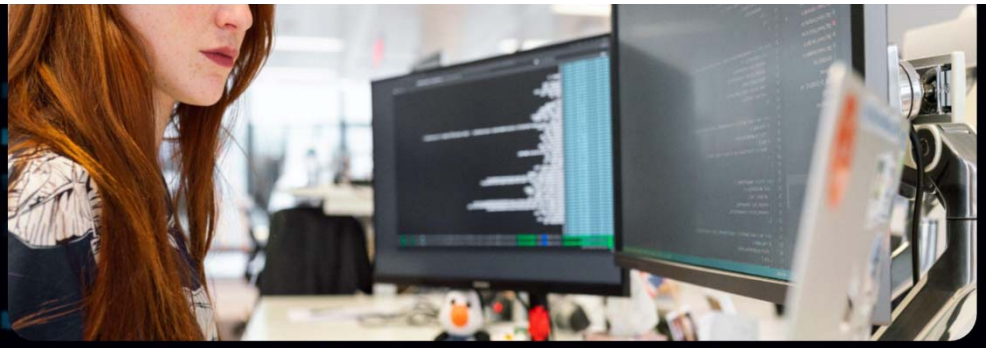
CYBERSECURITY AWARENESS MONTH

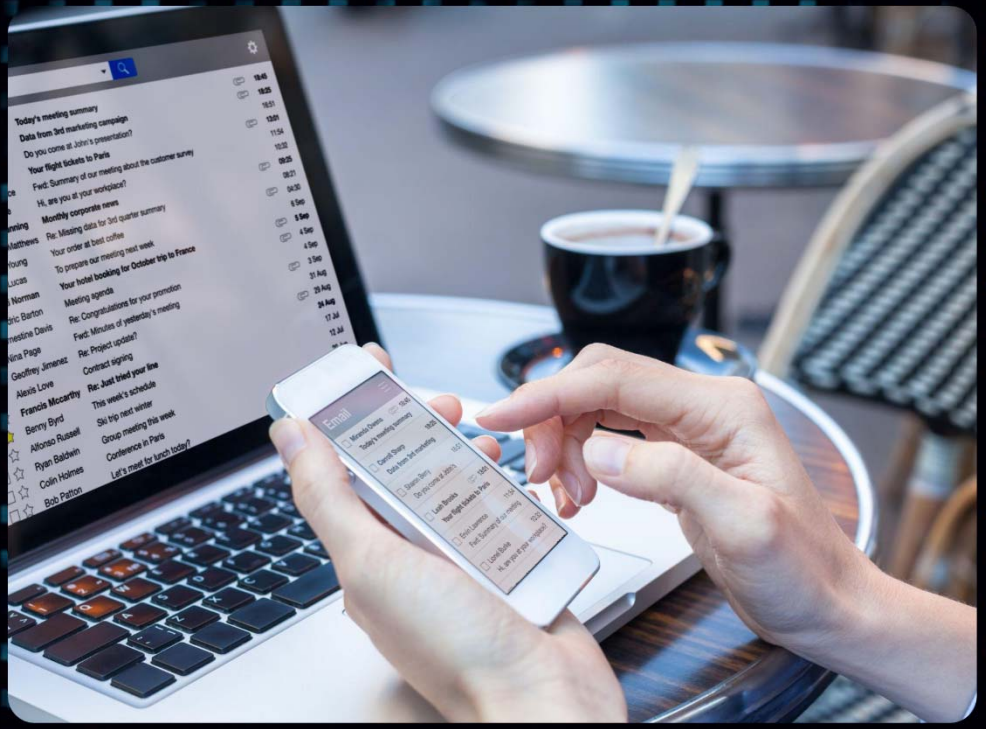
Clackamas Community College

SABY WARAICH
CIO | DEAN OF TECHNOLOGY

This year, we are focusing on

- Enabling multi-factor authentication
- Using strong passwords and a password manager
- Updating software
- Recognizing and reporting phishing





https://staysafeonline.org/programs/about-cybersecurity-awareness-month/

Mentimeter Exercise

Go to menti.com on a new browser page, your tablet or phone

Add in the Menti code

8972 9140

Always enable multi-factor authentication.

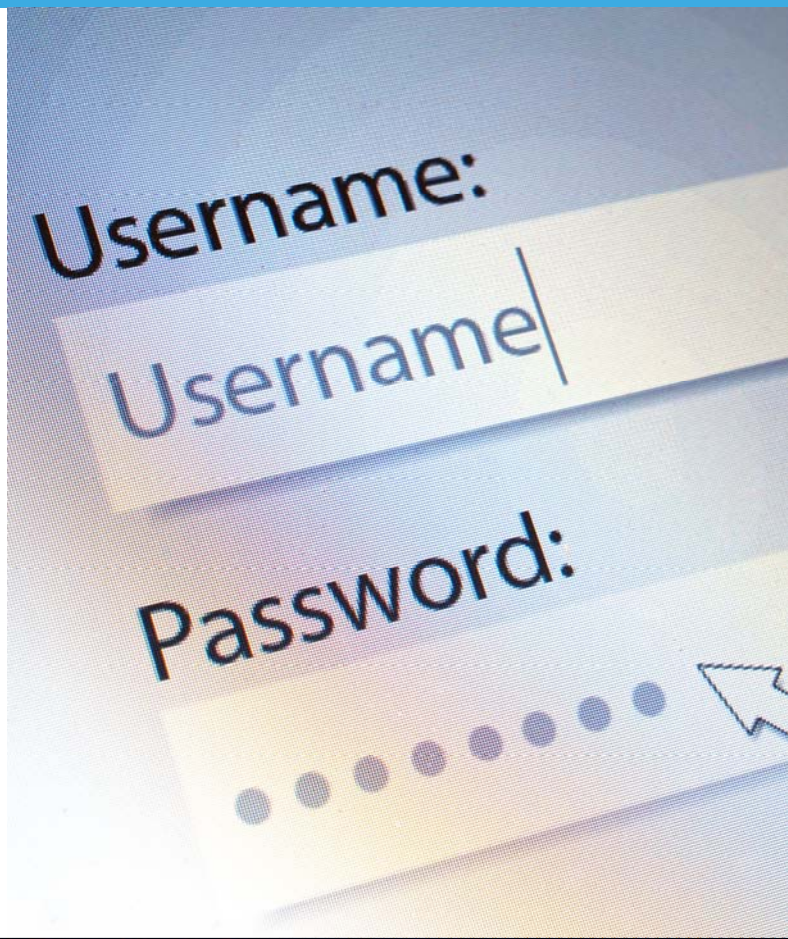
Also known as two-factor authentication and two-step verification. MFA can include:

- An extra PIN (personal identification number)
- An extra security question like, “What’s your favorite pet’s name?”
- An additional code either emailed or texted
- A biometric identifier like facial recognition or a fingerprint
- A unique number generated by an “Authenticator App”
- A secure token, which is a separate piece of hardware (like a key fob that holds information) that verifies a person’s identity with a database or system

LONG, UNIQUE, COMPLEX

No matter the account, all passwords should be created with these three words in mind:

- Long – At least 12 characters
- Unique – Never reuse passwords. Each account needs its own unique password
- Complex – Use a combination of upper- and lower-case letters, numbers and special characters. Some websites will even let you include spaces.



Recommendations for CCC Standard

- Passwords/passphrases must have a minimum length of 12 characters.
- Passwords/passphrases must contain both numbers and alphabetic characters. Complex password special characters allowed, but not required.
- Users are required to change passwords/passphrases at least every 90 days.
- Password/passphrase parameters must be set to require the new password/passphrase to be different from the previous 4 passwords/passphrases.
- First-time passwords/passphrases for new users and reset passwords/passphrases for existing users must be unique to each user and changed after the first use.
- Limit repeated access attempts by locking out the user ID after not more than 3 attempts.
- Once a user is locked out of their account, the account remains locked for a minimum of 30 minutes or until a system administrator resets the account.
- Automatic screen lock after 30 minutes of inactivity for Faculty or staff computers and 90 minutes for podium computers.

Clackamas Community College

DON’T TAKE A PASS ON PASSWORD MANAGERS.

Password managers not only let you manage hundreds of unique passwords for your online accounts, but some of the services also offer other advantages as well:

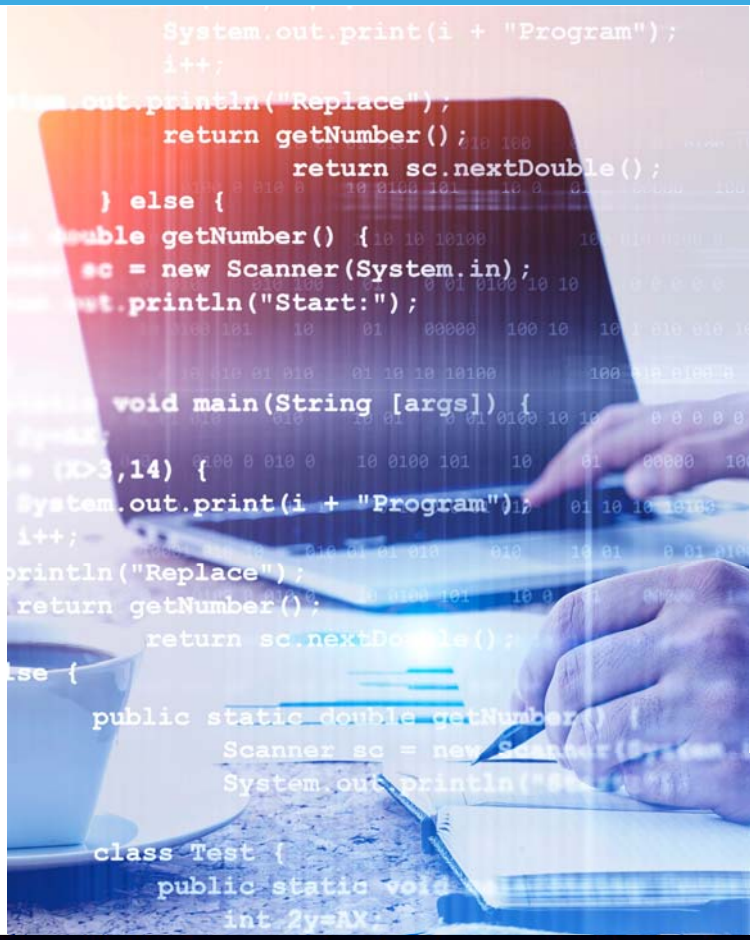
- Saves time
- Works across all your devices and operating systems
- Protects your identity
- Notify you of potential phishing websites

Update often.

Software updates fix general problems and provide new security patches where criminals might get in.

When downloading a software update, only get it from the company that created it. Hacked, pirated or unlicensed versions of software often contain malware and cause more problems than they solve.

Turn automatic updates on



See it so you don’t click it.

Here are some quick tips on how to clearly spot a fake phishing email:

- Contains an offer that’s too good to be true
- Language that’s urgent, alarming, or threatening
- Poorly-crafted writing with misspellings, and bad grammar
- Greetings that are ambiguous or very generic
- Requests to send personal information
- Urgency to click on an unfamiliar hyperlinks or attachment
- Strange or abrupt business requests
- Sending e-mail address doesn’t match the company it’s coming from

Get Involved

- Watch the assigned cybersecurity training this month
- Email on 10/3/2022 -> clackamascommunitycollege@securityiq-notifications.com

Clackamas Community College

Hello Saby,

You have been enrolled in the optional **Security Awareness Training for Higher Education - Fall Term** course, courtesy of Clackamas Community College. Please take this opportunity to become more aware of information security best practices. This training will be available for the next 44 days.

Start your training

Thank you,

ITS Team at Clackamas Community College

Get Involved

- Watch the assigned cybersecurity training this month
- Implement best practices as outlined in this presentation – examples:
  - Are your passwords long, unique and complex?
  - Do you have MFA enabled?
  - Do you know how to successfully report phishing messages?
- Download/review the posters, newsletters and emails sent throughout the month
- Share these tips on social media and/or with your family

Information Security is everyone's responsibility!!

Questions?