



Romel Cabiling ▾



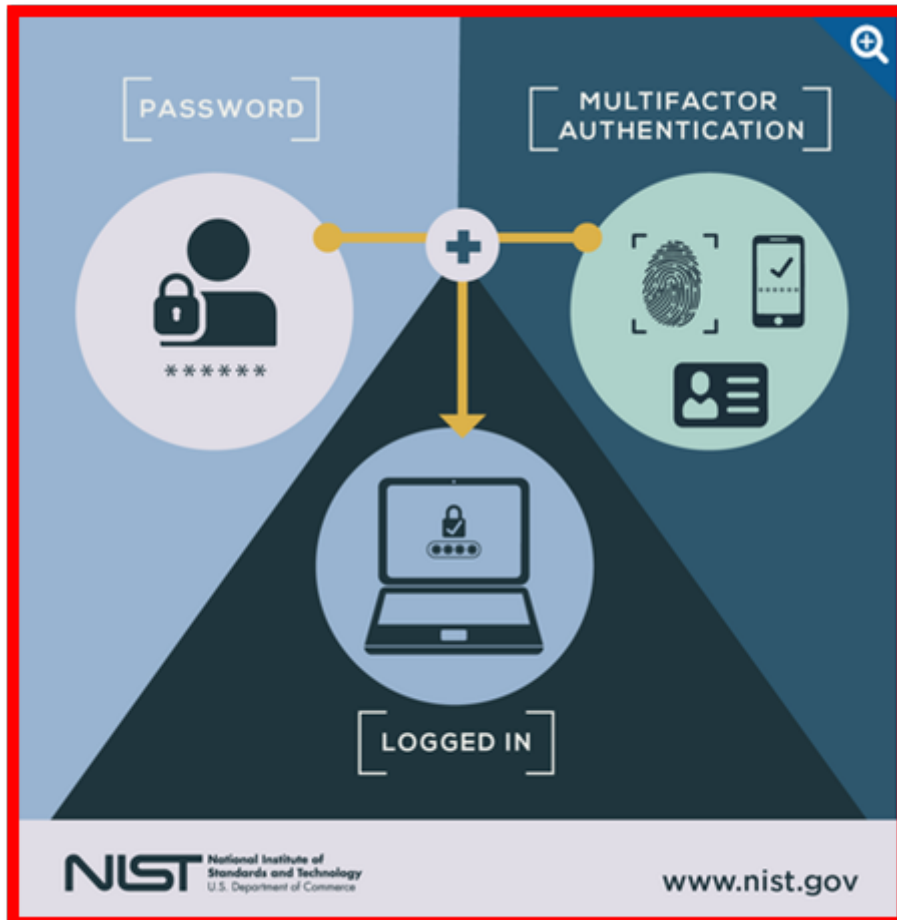
Home

Home > My courses > Network Attacks: Detection, Analysis & Counter... > 16 Multi-Factor Authentication (Mfa)
> Lesson Proper for Week 16

Lesson Proper for Week 16

IV. DEVELOPMENT OF THE LESSON

MULTI-FACTOR AUTHENTICATION (MFA)



Multi-factor Authentication (MFA)

- An authentication method that requires the user to provide two or more verification factors to gain access to a resource.
- A security technology that requires multiple methods of authentication from independent categories of credentials to verify a user's identity for a login or other transaction.
- Sometimes referred to as two-factor authentication or **2FA**, is a security enhancement that allows you to present two pieces of evidence – your credentials – when logging in to an account.

Your credentials fall into any of these three categories:

- o Something you know (like a password or PIN)
- o Something you have (like a smart card)
- o Something you are (like your fingerprint)

Your credentials must come from two different categories to enhance security – so entering two different passwords would not be considered multi-factor.

IMPORTANCE OF MULTI-FACTOR AUTHENTICATION (MFA/2FA)

Two-factor authentication (2FA) is the foundational element of a zero trust security model. In order to protect sensitive data, you must verify that the users trying to access that data are who they say they are. 2FA is an effective way to protect against many security threats that target user passwords and accounts, such as phishing, brute-force attacks, credential exploitation and more.

Let's say you use a username and password to complete primary authentication to an application. That information is sent over the Internet (your primary network).

So why does it matter? If a remote attacker is able to tap into your computer via your Internet connection, they can steal your password, and your second form of authentication — if both are delivered over the same channel.

Without your physical device, remote attackers can't pretend to be you in order to gain unauthorized access to corporate networks, cloud storage, financial information, etc. stored in applications.

By integrating two-factor authentication with your applications, attackers are unable to access your accounts without possessing your physical device needed to complete the second factor.

FACTORS OF AUTHENTICATION

a. Knowledge Factor

The knowledge factor verifies identity by requesting information only an individual user would know. The most common example of a knowledge factor of authentication is a **password**. A user's password should be private only to them, allowing them to use it as a method to confirm their identity.

b. Possession Factor

Possession factors verify the identity of a user by requiring proof of information that only the user should possess. **Tokens** are a commonly used possession factor of authentication. These tokens generate a rotating passcode that users must physically carry on their person.

c. Inherence Factor

Inherence factors of authentication verify the identity of a user by using attributes that would belong only to that user. **Fingerprint scanning** is the most obvious inherence factor used today.

Fingerprints are unique to individuals, so many organizations use them as a way to confirm who their users are. In addition to fingerprints, there are many other inherence factors used today: voice, handprints, face recognition, and more.

d. Location Factor

Location factors of authentication confirm the identity of a user based on their location in the world. If a user had registered an account in one country, for example, and suddenly there are login attempts from another, location factors could trigger and attempt to verify the identity of the new user. Many location factors are based on the IP address of the original user and compares the address to that of the new attempt to access information.

e. Time Factor

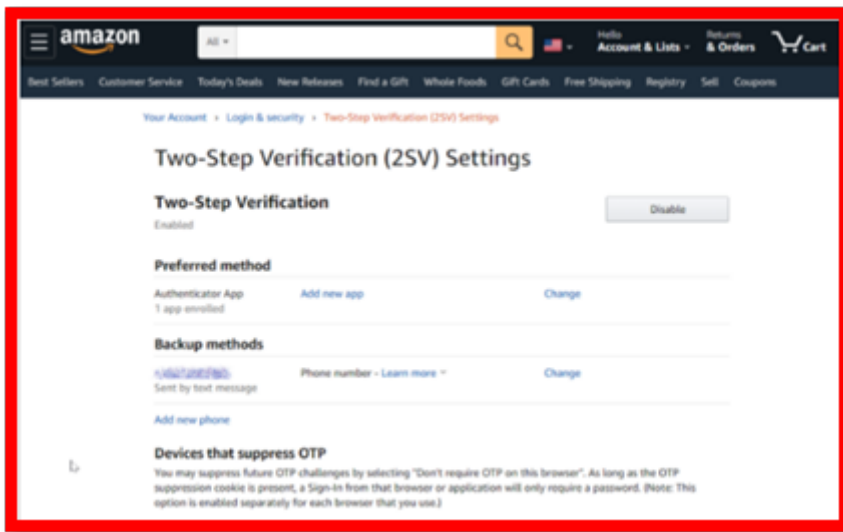
Time factors of authentication verify the identity of a user by challenging the time of the access attempt. This is based on the assumption that certain behaviours (like logging into a work computer) should happen within predictable time ranges. If an attempt to access a platform happens outside of the usual time range, the attempt can be challenged or terminated until a user can verify their identity.

LIST OF SERVICES WITH MULTI-FACTOR AUTHENTICATION (MFA/2FA)

ABILITY

The following is not a complete list of services with 2FA ability, but we cover the major services everyone tends to use, and walk you through the setup. Activate 2FA on all of these and you'll be more secure than ever.

1. AMAZON Two-step Verification



Amazon added 2FA support late in 2015 and it's pretty important to turn on, as Amazon has its fingers in many pies, like Comixology, Audible.com, and sites that use Amazon for payments—all tied to your credit card.

2. APPLE Two-Factor Verification



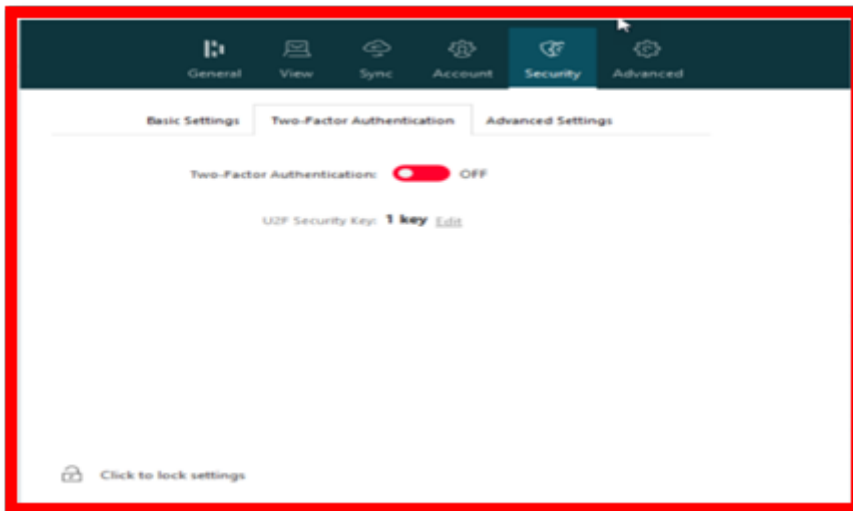
Your Apple ID is a big part of your life if you're an iOS or Mac user. It's important for not just access, but also storage via iCloud; purchases like movies, books, and apps; and memberships like Apple Music and Apple TV+.

You'll have to answer two of your three pre-set security questions and re-confirm your credit card on the account to get into the setup. Then you have to enter a valid phone number to get a text or phone call (even if it's the number already on the phone you're using for setup). If it is the same phone, the six-digit code will be entered automatically when it arrives, or just type it in.

After that, signing into anything with the Apple ID should generate a code on the device used for setup. Apple also supports app-specific passwords.

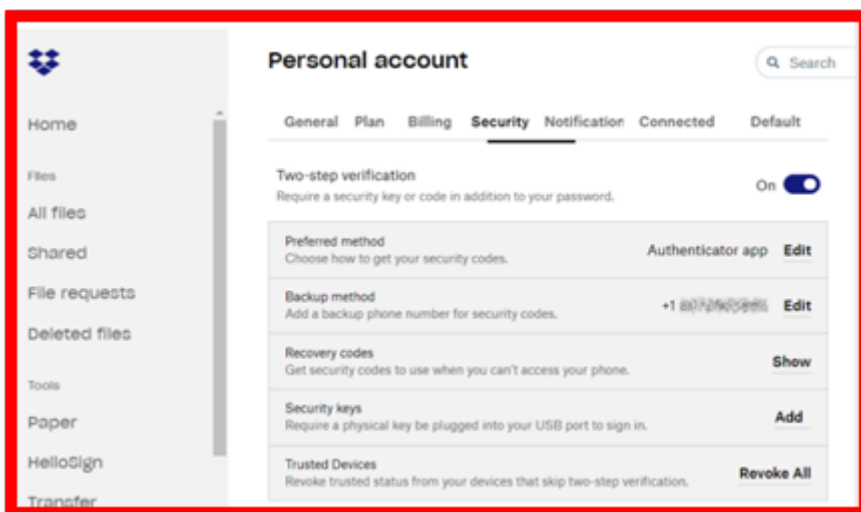
Note that once Apple 2FA is activated for two weeks, you can't turn it off. "Certain features in the latest versions of iOS and macOS require this extra level of security, which is designed to protect your information," Apple says.

3. DASHLANE Two-Factor Authentication



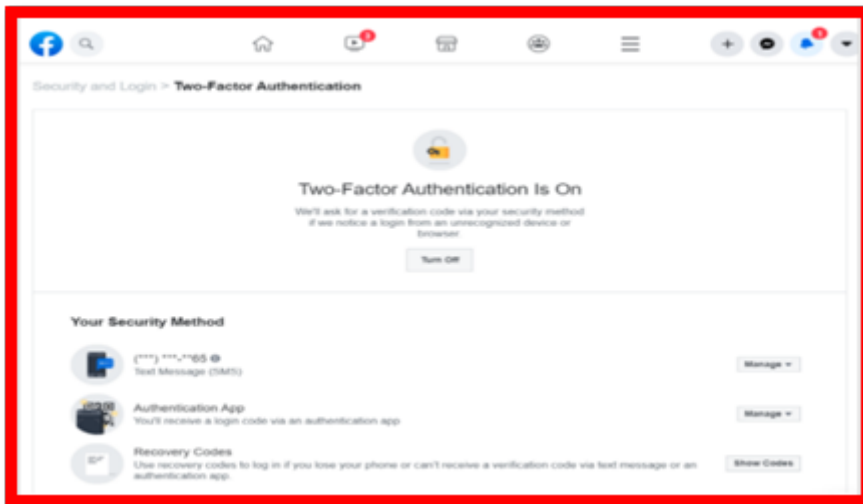
A password manager favourite, Dash lane also supports 2FA. You have to turn it on via the desktop using the software for Windows or macOS, and you'll need a separate authenticator app on your smartphone to scan the QR code.

4. DROPBOX Two-Step Verification



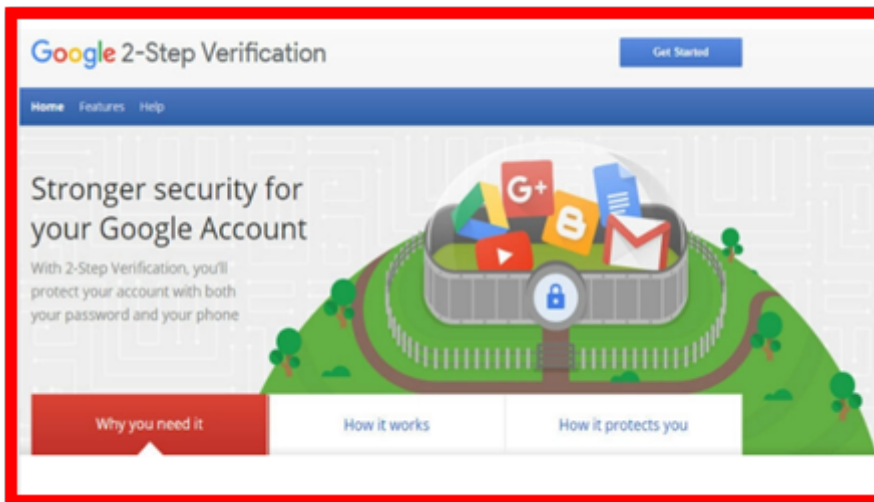
Dropbox on the desktop website has a tab called Security. It's where you go to check how many current sessions are logged in and devices are using the account, to change the password, and, of course, turn on two-step verification. Toggle it to on, enter a password, and you'll be asked if you want to get security codes via SMS text message or via a mobile authenticator app.

5. FACEBOOK Two-Factor Authentication



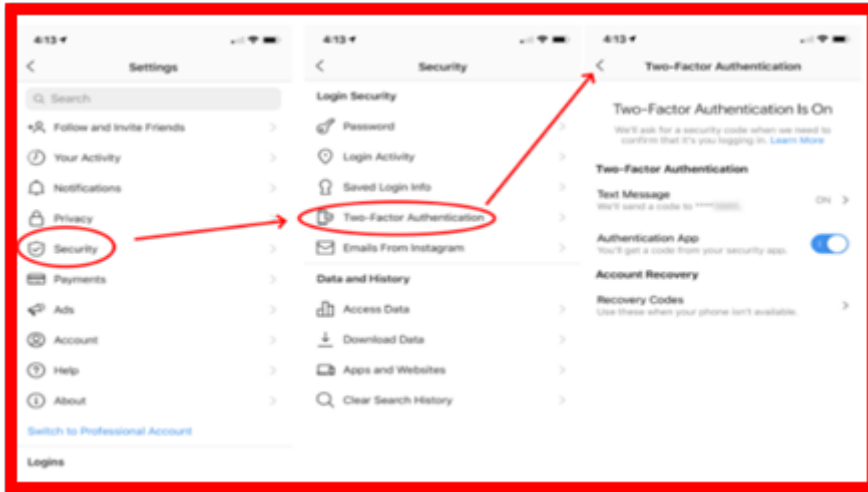
Facebook offers App Passwords, a one-time password to access your Facebook account via any third-party app or service. If you log out of that app or service and need to go back in, you'll have to generate a new, unique app password. This is necessary for older devices.

6. GOOGLE Two-Step Verification



Google calls its system 2-Step Verification. It's all about identifying you via phone. When you enter a password to access your Google account for almost any service, if 2-Step Verification is on, there are multiple options to get that second step. First among them now: the Google Prompt. You simply add your smartphone to your account, make sure the Google search app is on the phone, and at login, you can go to the phone and simply acknowledge with a tap that you are the one signing in. Easy.

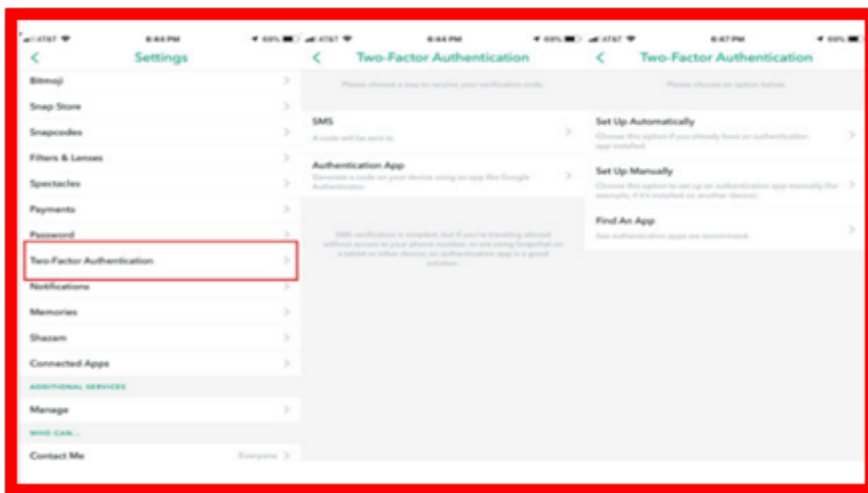
7. INSTAGRAM Two-Factor Authentication



Facebook-owned Instagram has offered two-factor authentication since 2016. The app also offers a list of five recovery codes for use in the future to turn off 2FA or get access via other devices. It even offers to take a screenshot of them to add to your camera roll; you can always re-access them in the app as well.

Option one: turn on Text Message and add your phone number (include the country code, because Instagram is everywhere). You'll get a confirmation code via SMS text message. Enter it. Option two: turn on Authentication App. The app will walk you through the steps to set it up (since you can't exactly scan a QR code from your mobile phone while using the app on your mobile phone.)

8. SNAPCHAT Two-Factor Authentication



Snapchat is a mobile-only service, so the only way to set up 2FA is via the mobile app. Snapchat warns you that if you lose access to your method for generating a login code (aka, your phone), you could get locked out of your Snapchat account. If you're okay with that, proceed with setup, and select whether you want to receive a code via text or an authenticator app (you can have both active simultaneously).

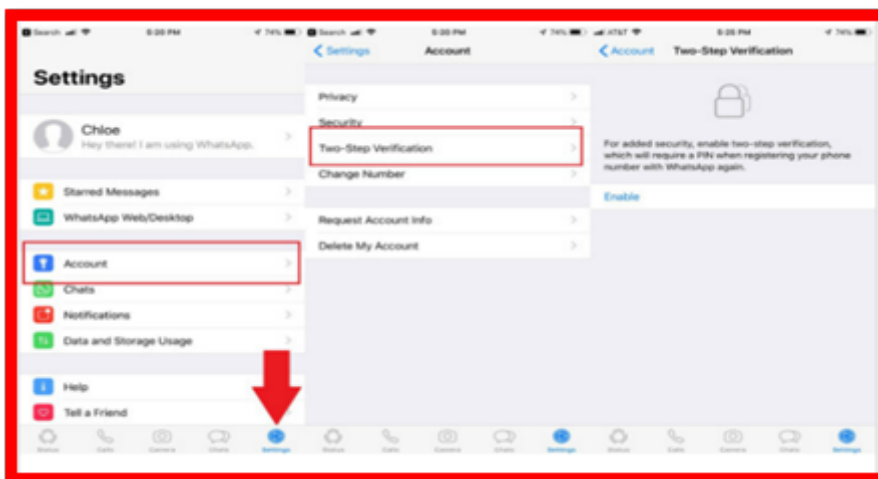
9. TWITTER Two-Factor Authentication



Twitter will generate backup codes for when you lose a device, and temporary passwords to use one time when logging in at services/places/times you also can't get a regular 2FA code.

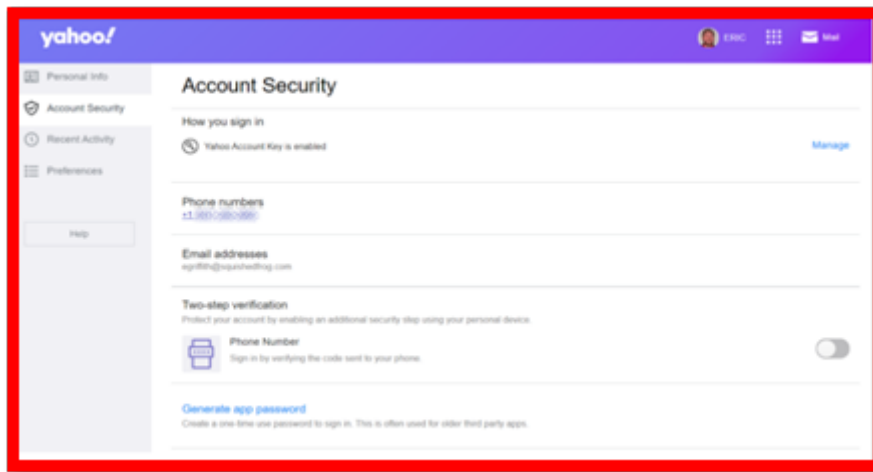
You can also use the Twitter app itself as an authentication app. Click Login code generator to get a six-digit number that updates every 30 seconds, which can help when signing into third-party sites with your Twitter credentials.

10. WHATSAPP Two-Step Verification



WhatsApp introduced end-to-end encryption as well as two-step authentication. If you later sign out or log in with a different device, WhatsApp will text you a code, and you'll have to re-enter the PIN as well. You can go in to the app to change the PIN or your email any time.

11. YAHOO Account Key or 2-Step Verification



The Yahoo Account Key is the next best thing. It's very similar to Google Prompt. If you have any Yahoo app on your phone, Yahoo Account Key can send a notification to it directly. You get the notification, push a button to confirm it's you, and that's it—

No codes or passwords to enter. (If you don't have a Yahoo app on your mobile device, Yahoo can text or email you an 8-letter code.) When/if you activate Yahoo Account Key, Yahoo deactivates two-step verification, and vice versa, as Account Key must be turned off to allow two-step verification.

AUTHENTICATION THREATS

The need for two-factor authentication has increased as companies, governments, and the public realize that passwords alone are not secure enough to protect user accounts in the current technical landscape. The most common threats include:

1. Stolen Passwords. A traditional password can be used by anybody who gets their hands on it. If a user writes down their password on a pad of paper, for example, that password can be stolen to gain access to an account.

2FA, by contrast, validates the user with a second device after a password is entered.

2. Phishing Attempts. Hackers will often send emails that include links to malicious websites designed to either infect a user's computer or convince them to enter their passwords. Once obtained, a password can be used by whoever manages the hacking attempt.

2FA fights phishing by adding a second layer of validation after the password has been entered.

3. Social Engineering. Hackers will often simply manipulate users into giving up their passwords. By posing as an IT professional at the user's company, they can earn the trust of the user before asking for login credentials.

2FA protects against this by validating the location and IP of every login attempt after a password has been entered.

4. Brute-Force Attacks. In a brute-force attack, a hacker randomly generates passwords for a specific computer until they land on the correct sequence.

2FA's second layer of protection requires a login attempt to be validated before granting access.

5. **Key Logging.** Even if a user hasn't written down their password, hackers can use malware to track and copy a user's password as they type. Hackers track every keystroke and store the password to be used later.

The second layer of validation in 2FA lets a user ensure that the login attempt is their own, even if their password has been compromised.

TYPES OF MULTI-FACTOR AUTHENTICATION (MFA/2FA)

§ **SMS two-factor authentication** validates the identity of a user by texting a security code to their mobile device. The user then enters the code into the website or application to which they're authenticating.

§ **The Time-Based One Time Password (TOTP) 2FA method** generates a key locally on the device a user is attempting to access. The security key is generally a QR code that the user scans with their mobile device to generate a series of numbers. The user then enters those numbers into the website or application to gain access. The passcodes generated by authenticators expire after a certain period of time, and a new one will be generated the next time a user logs in to an account. TOTP is part of the Open Authentication (OAUTH) security architecture.

§ **Push-based 2FA** improves on SMS and TOTP 2FA by adding additional layers of security, while improving ease of use for end users. Push-based 2FA confirms a user's identity with multiple factors of authentication that other methods cannot. Duo Security is the leading provider of push-based 2FA.

§ **Universal 2nd Factor (U2F) tokens** secure two-factor authentication by using a physical USB port to validate the location and identity of a user attempting to login. To use a U2F token, a user inserts the token into their device and presses the button located on the top of the device. Once the token is activated, the user enters their PIN and gains access to their accounts.

INDUSTRIES THAT USED MULTI-FACTOR AUTHENTICATION (MFA/2FA)

1. **Healthcare organizations** are concerned about securing patient data and personally identifiable information (PII). The healthcare industry must also securely enable their clinicians and physicians to access patient data, at anytime, anywhere - sometimes from their own personal devices.

2. The **banking industry** uses 2FA to protect against the many hacking attempts made on their internal and clients' systems. Duo's push-based authentication system has helped many large banks improve their resiliency against such attacks. It is important for security teams to know which users and devices are accessing their systems.

*Duo's push-based authentication adds a second layer of security to your online accounts. Verifying your identity using a second factor (like your phone or other mobile device) prevents anyone but you from logging in, even if they know your password.

3. The **media industry** spans across radio, television, social media, film, and more. 2FA helps media companies by allowing users to access the data necessary to meet publishing deadlines.

By securing IT infrastructures across companies and state lines, Duo's two-factor authentication technology gives media companies the ability to validate users' identities whenever a login is attempted.

4. **Social media platforms and agencies** use 2FA to protect the personal data of billions of users worldwide. To protect these users, social media companies like Facebook use Duo's push-based authentication to shield their developers from hacking attempts when working on the company's internal networks.
5. **Higher education institutions** manage vast amounts of sensitive user data involving finance, healthcare, PII, and more. This valuable data has historically made institutions prime targets for hacking and malicious breaches of security.
6. Colleges and universities use 2FA to secure the mobile devices and personal computers of students, faculty and staff. Securing these devices helps combat malicious actors by authenticating the identity and location of every login attempt.

◀ Preliminary Activity for Week 16

Jump to...



Analysis, Application, and Exploration for Week 16 ▶



Navigation

Home



Dashboard

Site pages

My courses

Capstone Project 1

Network Attacks: Detection, Analysis & Counter...

Participants

General

12 - Midterm Examination

14 Search Engines

15 Encryption And Certificates


16 Multi-Factor Authentication (Mfa)

 Preliminary Activity for Week 16

 **Lesson Proper for Week 16**

 Analysis, Application, and Exploration for Week 16

 Generalization for Week 16

 Evaluation for Week 16

 Assignment for Week 16

Ojt/Practicum 1

Social And Professional Issues

Fair Warning

NOTICE: Please be reminded that it has come to the attention of the Publishing Team of eLearning Commons that learning materials published and intended for ***free use only by students and faculty members within the eLearning Commons network were UNLAWFULLY uploaded in other sites without due and proper permission.***

PROSECUTION: Under Philippine law (Republic Act No. 8293), copyright infringement is punishable by the following: Imprisonment of between 1 to 3 years and a fine of between 50,000 to 150,000 pesos for the first offense. Imprisonment of 3 years and 1 day to six years plus a fine of between 150,000 to 500,000 pesos for the second offense.

COURSE OF ACTION: Whoever has maliciously uploaded these concerned materials are hereby given an ultimatum to take it down within 24-hours. Beyond the 24-hour grace period, our Legal Department shall initiate the proceedings in coordination with the National Bureau of Investigation for IP Address tracking, account owner identification, and filing of cases for prosecution.

Graduation Announcement



**BESTLINK COLLEGE
OF THE PHILIPPINES**

ANNOUNCEMENT

Due to the insistent demand of BCP graduates and alumni and the IATF pronouncement of the low Alert Level Status, and in coordination with the DepEd and CHED, the BCP Administration is happy to announce that face-to-face graduation rites will proceed as scheduled.

<u>Level</u>	<u>Date of Graduation</u>	<u>Venue</u>	<u>Graduation Fee</u>	<u>Downpayment</u>
SHS	July 16, 2022	MV Campus	P 1,000.00	P 200.00
College	July 10, 2022	PICC	P 4,000.00	P 500.00

Balance must be paid two (2) weeks before the date of graduation.



**BESTLINK COLLEGE
OF THE PHILIPPINES**

SCHEDULE GRADUATION PHOTOSHOOT

**College Department Batch 2021-2022
(Main Campus)**

May. 23 & 30 - CRIM

May. 24 & 31 - EDUC

May. 25 & Jun. 01 - BSBA/BSOA/BSAIS/ENTREP

May. 26 & Jun. 02 - BSIT/BLIS/BSP/BSCpE

May. 27 & Jun. 03 - BSHM/BSTM

"Be trained to be the best, be linked to success"



More information call us (028)4420-8601 | (028)8518-8050





**BESTLINK COLLEGE
OF THE PHILIPPINES**

SCHEDULE GRADUATION PHOTOSHOOT

Bulacan Branch Batch 2021-2022

May 28

8am - 12nn: Senior High School

12nn - 5pm: College Department

"Be trained to be the best, be linked to success"



More information call us (028)4420-8601 | (028)8518-8050



Activities



Assignments



Forums



Quizzes



Resources

Bestlink College of the Philippines
College Department

Powered by [eLearning Commons](#)