

Be Unique!

Your password is easier to hack than you think.

Over 99% of passwords can be found within the top 100. Most commonly used passwords **LEAK YOUR INFORMATION MORE SURELY** by creating a password that is complex to all you remember to you!

Here's How

- 1 Don't use your birth department for you - it has been a great way to guess email accounts, login pages - then take the last four digits.
- 2 Avoid using the same password with other accounts, email, and social networks.
- 3 Remember personal names. They often don't change for different accounts. If you're using a website as an employer or school, use a password that is unique to that account, not your birthday.

➔ Mix & Match Acronyms With Numbers
➔ NUMBERS
➔ BIRTH DATES

Learn more at security.ucop.edu

1

Different Keys for Different Places

Using the same password for multiple accounts opens the door to greater losses.

Use different passwords for different accounts, just as you use different keys for your car, home, and mailbox.

DO NOT REUSE — use a unique password for every online account.

Learn more at security.ucop.edu

2

Always CHECK before you CLICK!

Don't help cybercriminals steal your information.

TARGETED EMAILS from hackers will look legitimate at first glance.

Make sure the email is **GENUINE** before you click on any links!

What To Check For

- 1 Look for grammatical spelling or grammar errors.
- 2 Trust any email you didn't expect to receive with suspicion.
- 3 Check for misspellings, word choice and links that don't match the sender.
- 4 Hover over links to see if the web address is legitimate and relates to the email content.

Verify any email that asks for personal information by independently looking up the sender's contact information.

Learn more at security.ucop.edu

3

Panicking Over a Lost Phone?

You should be. Help us help you protect your privacy.

You never know who is browsing your photos, laughing at your texts, or reading your emails on your lost phone.

REPORT ANY LOSS so that Information Security can work with you to protect both your information and the company's information.

Learn more at security.ucop.edu

4

"Can you hold the door? I forgot my badge today..."

It's okay to say "no" to badge-surrender!

"I wish I could, but I don't want to accidentally let a shark in. I'll be at the front desk can make you a temporary badge!"

Check in with the front desk or Security if you have forgotten your badge. Politely ask unknown colleagues to do the same.

REPORT ANY SUSPICIOUS ACTIVITY so that Security can better protect the work environment.

Learn more at security.ucop.edu

5

Hello? Who's Calling?

Keep your personal information safe from con artists.

An **UNFAMILIAR VOICE** is calling with an important request for information.

How do you know they are who they say they are?

Don't be tricked into giving personal information over the phone. If you don't recognize the voice, don't answer any personal questions. Instead, **INDEPENDENTLY VERIFY** their phone number, and call them to be sure you are talking to who you think you are!

Learn more at security.ucop.edu

6

Is someone monitoring you?

While convenient, public Wi-Fi is not so secure. Be careful how you work and surf when connected.

The Eye & Sea Cafe

Be Safe on Public Wi-Fi

- Encrypt your data by using your company-provided VPN.
- Be careful of who can see your screen and work.
- Be cautious of coffee shops, airports, buses, trains, libraries, and public areas near the workplace.

PLAY IT SAFE! Save confidential tasks for when you're connected to a secure network.

Learn more at security.ucop.edu

7

Do You Know Where Your Files Are Really Stored?

Make sure there are no holes in your boxes.

What could be **LOOKING?**

Internet sites that promise free file storage appear convenient but they don't protect your information.

Put your files in your company's **SECURE STORAGE!**

Learn more at security.ucop.edu

8