PASSWORDS ARE LIKE SNOWFLAKES

They should be unique.

Never use the same password for your work and personal accounts!

D2 | CYBERSECURITY

PASSWORDS ARE LIKE SOCKS

They should be changed often.

KEEP YOUR PASSWORDS SAFE BY FOLLOWING THESE EASY TIPS:

- Don't share them
- Don't leave them out in the open
- Create longer and stronger passwords
- Never use the same password for different accounts

If you think your password has been compromised, change it immediately!

D2 | CYBERSECURITY

PASSWORDS ARE LIKE GERMS

Don’t share them with your friends.

Don’t spread your passwords around! Keep them to yourself.

D2 | CYBERSECURITY

Don’t fall hook, line, and sinker for

PHISHING SCAMS

Phishing attacks only need to deceive a single person to be successful! With one click, you could hand complete control of your network over to an intruder. Always carefully investigate all links and attachments while checking emails.

D2 | CYBERSECURITY

Check your incoming emails for SPELLING ERRORS!

Spelling or grammatical errors within an email are indicators of a potential phishing attempt. When in doubt, ask your IT security team to investigate the message.

D2 | CYBERSECURITY

Public Wi-Fi isn't

SAFE WI-FI!

Free public Wi-Fi can be useful, but is it safe? Always protect your device by enabling its VPN features before connecting. Avoid handling private information until you're on a secure network.

D2 | CYBERSECURITY

Cybersecurity starts with YOU!

It is your responsibility to understand, enact, and maintain all current security fundamentals. Stay informed of industry best practices by completing all assigned security awareness training.

D2 | CYBERSECURITY

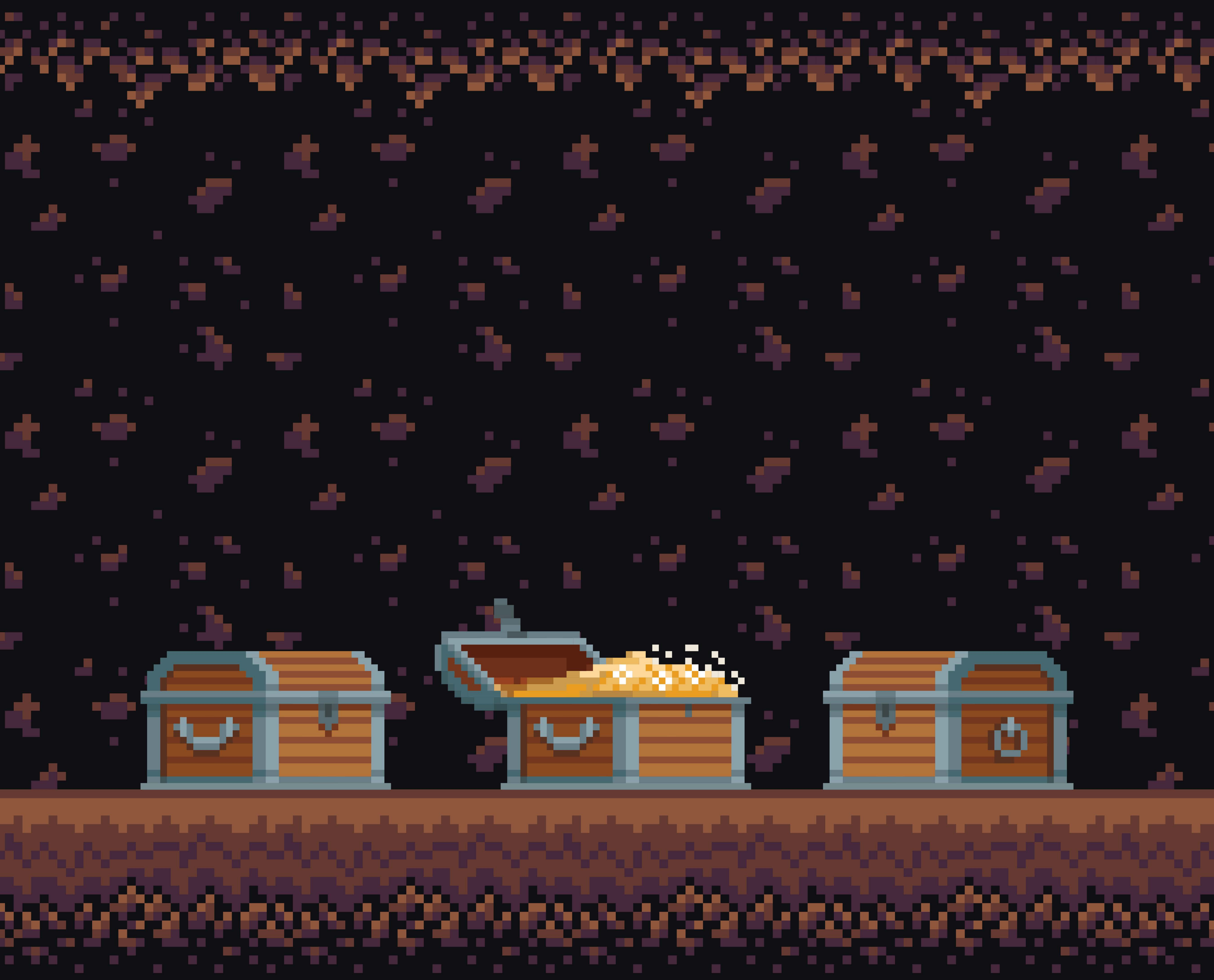
Close the door on intruders!

Mitigating security threats requires strong offline awareness skills. Always verify that office doors close and lock behind you. Never let a stranger inside without verifying their identity!

D2 | CYBERSECURITY

PASSWORDS ARE LIKE TREASURE

Keep them secure in a safe place.



Use a password vault/manager that supports multi-factor authentication.

D2 | CYBERSECURITY

CYBERSECURITY IS A SHARED RESPONSIBILITY

USE SECURE PASSWORDS

A PASSWORD is important – keep it SAFE and Unique.

KEEP YOUR PASSWORD SAFE AND UNIQUE BY FOLLOWING THESE EASY TIPS:

DEVELOP strong passwords by using a combination of words, numbers, and symbols. Be sure to use both upper-case and lower-case letters

CREATE a passphrase and make it relevant. For example, if you're "About to Use a Shopping Site", your passphrase could be "ABT2_uz_$h0pping"

USE a different password for every unique account, such as work, banking, and email

DISABLE the "Save Password" feature in your Internet browser settings

If you think your password has been compromised, change it immediately!

D2 | CYBERSECURITY

CYBERSECURITY IS A SHARED RESPONSIBILITY

DON'T TAKE THE BAIT

- If someone asks you for information, always confirm that you know the sender and source of the message before responding
- Do not open attachments or click on links from untrusted sources or unknown senders
- Don't fall victim to false urgency or fake threats!

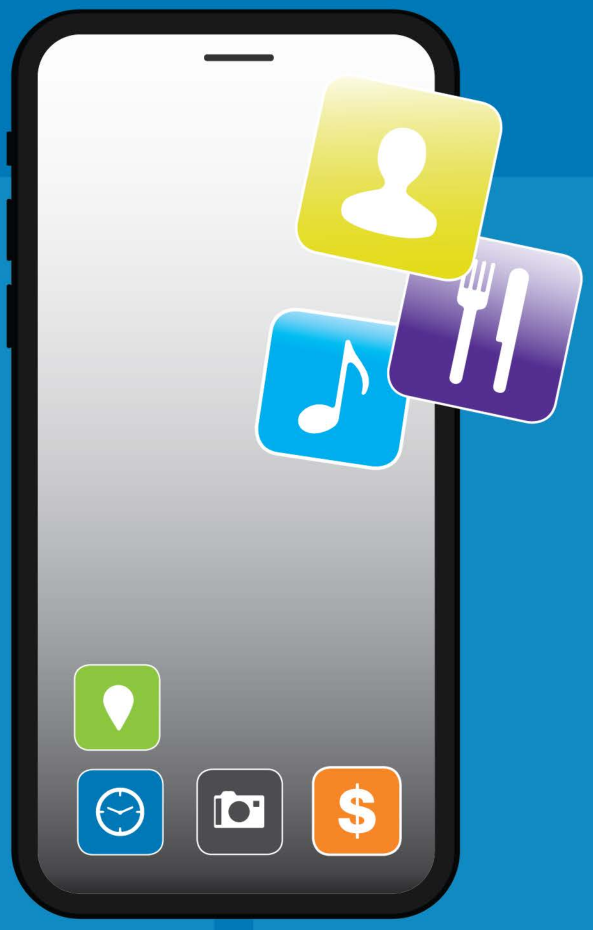
IF A MESSAGE SEEMS TO BE UNSAFE, CALL THE SENDER OR SEND THEM A NEW EMAIL TO CONFIRM

D2 | CYBERSECURITY

★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★

CYBERSECURITY IS A SHARED RESPONSIBILITY

PROTECT YOUR SMARTPHONE



✓ DO'S

- Make sure the operating system and software are up-to-date at all times
- Check the feedback from other users before installing any program from an app store
- Do not give apps permission to access your contacts, camera, or microphone. The less they have access to, the better
- Close any apps that are not in use
- Turn off Bluetooth and other connections when not in use

✕ DON'TS

- Use your phone without a password
- Use third-party app stores or suspicious sites to download apps
- Leave your mobile device unattended in public places
- Hack or jailbreak your phone
- Respond to strange texts
- Store sensitive information on your phone

D2 | CYBERSECURITY

CYBERSECURITY IS A SHARED RESPONSIBILITY

CONNECT WITH CARE

- Keep your devices updated with the latest system and application patches.
- Assume that any public, unprotected Wi-Fi connection is not secure. If it doesn't require a password to connect, assume it is not SAFE.
- Do not log into an account that contains private information, such as your email or bank account, while using public Wi-Fi.
- Consider turning off device features when you are not actively using them.

D2 | CYBERSECURITY