Domain 7 · Safety and Security · Day 3

Digital Safety and Security

09

Security isn't a setting you turn on once — it's ongoing habits, because attackers work every moment.

IC3 GS6 · DOMAIN 7 | 75 MIN | DAY 3

Terms you will need shortly

Five terms before any explanation — Pre-training

Malware

Software that gets in without permission and does harm

Phishing

A message posing as a trusted source to get something from you

2FA

Two factors from two different categories

VPN

A tunnel that encrypts your connection on a network you don't trust

Remote Wipe

Erasing a device remotely after you lose it

What you take away from this unit

Four abilities you apply on your own devices in the room.

01 **You see the threat map**

Human-facing, software-based and physical — **and the first is the most common**.

02 **You build a passphrase and turn on 2FA**

Length you can remember, and a second factor that stops anyone who stole your password.

03 **You handle public networks**

You know what not to do, and when to go back to your cellular data.

04 **You protect your device before you lose it**

Lock, encryption, backup, tracking and remote wipe — five layers.

Three layers — and the first isn't technical — Threat layers



1. Human-facing — **phishing and social engineering**, aimed at you, not your device.
2. Software-based — viruses, worms, Trojans, ransomware, spyware and keyloggers.
3. Physical — theft, loss and damage; the result is data lost along with the device.
4. The first layer is the most common and the least technical — so that is where you start.

For an ordinary user, the biggest threat is not a skilled hacker but a message that seems to come from a source they trust.

Security is ongoing habits — not a to-do list you finish.

Attackers work every moment, faster than anyone can adjust settings.

Four signs that give away a scam message

Sign	How it shows up
False urgency	“Within 24 hours,” “Final warning” — to keep you from checking
A link that asks you to log in	Instead of you signing in through the official app
A request for data the organization doesn't ask for	**Your password, verification code or card number**
An offer too good to be true	A prize, a tax refund or a gift card

Recall

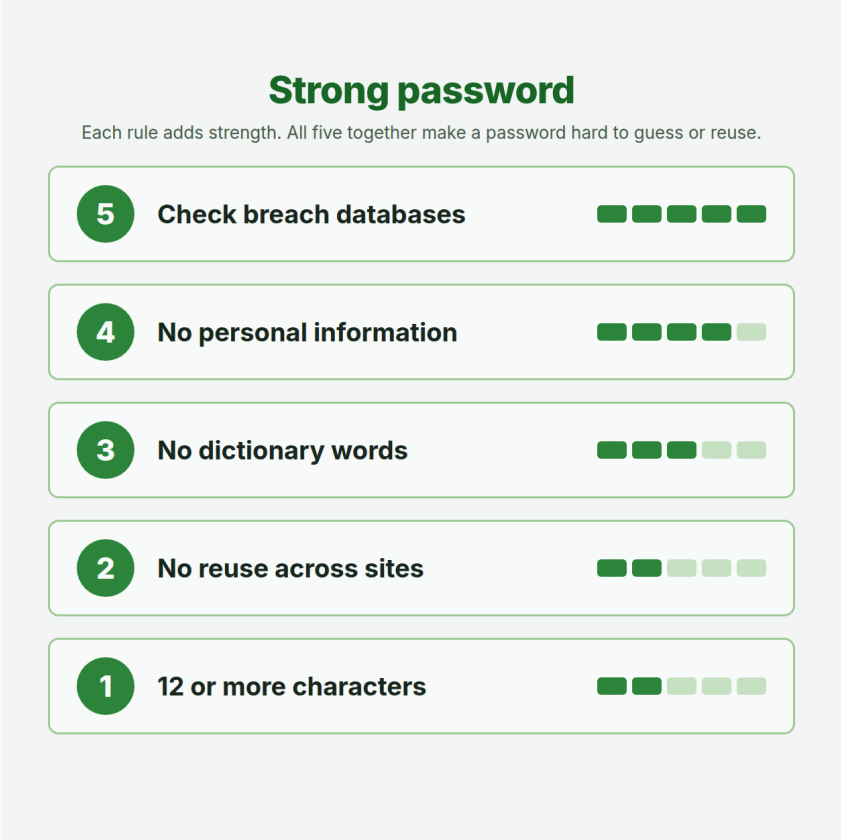
Close the book: what is the difference between a virus and a worm?

Which one needs you to do something?

And which one spreads on its own?

Two minutes, then we hear two answers.

Length before complexity — Password strength



1. **12 characters or more** — length comes before every other property.
2. Never reuse it on two sites — one breach opens the rest.
3. No dictionary words, and no personal details your followers know.
4. Check it against breach lists — what has leaked is already known.

The practical fix: a passphrase built on a personal memory — long by nature, and easy for you alone.

Three categories — and two factors from two of them

That is all you need to understand about authentication.

01 **Something you know**

A password, a PIN, or the answer to a security question.

02 **Something you have**

Your phone, an authenticator app, or a physical key in your pocket.

03 **Something you are**

Your fingerprint or face — **the easiest day to day.**

04 **The rule**

Two factors from two different categories, not two factors from one category.

Second-factor types, by security and convenience

Type	Security	Note
Text message with a code	Medium	Easy, but open to SIM swapping
Authenticator app	High	**The best option for the ordinary user**
Physical key	Very high	Requires buying a key and carrying it with you
Fingerprint or face	High	The easiest day to day — and works as a second factor with a password

Unit myth: a network password protects you

The common belief — and why it's tempting

A café or mall network is safe as long as it asks for a password to join.

It's tempting because a password means “restricted,” and the mind reads restricted as protected.

The correction

A password controls who joins the network — it does not isolate the people on it from one another.

On the network you are surrounded by strangers who may intercept your unencrypted connection — and the network itself may be a fake twin with a similar name.

Six rules for any public network

The rule	Why
Confirm the official name	Ask a staff member — similar names are traps.
Don't do anything sensitive	No bank logins, no card numbers, no official email.
Check the padlock	A secure address shows a closed padlock beside it.
Use a trusted VPN	It encrypts your connection — and free ones often sell your data.
Turn off auto-connect	So your device never joins a network you didn't choose.
Prefer your cellular data	Especially for financial transactions — it is a network only you use.

Worked example: a money transfer in a café

You need to send money to your brother while you are in a café inside a mall.

01 **The mistake**

Connecting to the venue's network and opening your bank app straight away — a network everyone shares with you.

02 **The right move**

Turn off the public network and switch on your cellular data — then complete the transaction.

03 **Prevention**

Turn off auto-connect so your device stops joining networks without your permission.

The rule

Anything sensitive goes through your own network — public ones are for browsing, not money.

Five layers that protect your device before you lose it

Five layers across three moments: before the loss, always, and after it.

Before

Lock and encryption

A quick auto-lock, a six-digit code instead of four, and encryption turned on.

Always

Backup

The Unit 6 rule applies here — a device can be replaced, data cannot.

After

Tracking and wiping

Turn on “Find My Device” before you lose it; wipe its contents remotely if you are sure it will not come back.

Who does private browsing hide you from?

Hides

From your device

It does not keep your browsing history or cookies after you close the window — so whoever uses your device cannot see them.

Doesn't hide

From the network

Your service provider, the network owner and the websites themselves all see your activity as it is.

The right limit

A local hygiene tool, not an invisibility cloak — anyone who mistakes it for hiding has built their security on an illusion.

Your body is part of your digital security — The 20-20-20 rule



1. Every 20 minutes, look 20 feet (6 meters) away for 20 seconds.
2. Screen at eye level, back supported, wrists straight.
3. **Stand up and walk for a minute every 30–45 minutes** — the body was not designed for nonstop sitting.
4. Switch off devices an hour before bed — blue light disrupts sleep.

And raising your phone to eye level protects you from what the book calls “text neck.”

Complete the missing layer

The five layers — the last two share one step, and one is missing.

01 **Device locking**

A six-digit code, and auto-lock after 30–60 seconds of inactivity.

02 **?**

03 **Backup**

With the 3-2-1 rule from Unit 6 — a device can be replaced, data cannot.

04 **Tracking and remote wipe**

To locate it, or to wipe what is on it if it can't be recovered.

Now on your own: harden one account

The most important account you own — usually your email.

Turn on two-factor authentication for it now if it isn't already on. Then write a new passphrase built on a memory, and check: have you used it on another site? Is the recovery email protected just as well?

Time
12 minutes

Format
Solo, on your own device

Outcome
A genuinely hardened account

The unit's pillars

Four facts to carry into the next unit.

01 **The first threat is human-facing**

A message posing as a trusted source is more common than any malware.

02 **Length before complexity**

A long passphrase you memorize, never reused on two sites.

03 **Two factors from two categories**

What you know, what you have, what you are — and two from one category are not two-factor authentication.

04 **Public networks are for browsing**

And its password does not isolate you from the others on it.

Terms the exam questions turn on — Exam terms

Cover the meaning and recall it — for every term you have met.

Virus vs Worm

Needs you to run it, versus spreads on its own

Phishing · Smishing

Impersonation by email, and by text message

Ransomware

Encrypts your files and demands a ransom

2FA vs MFA

2FA: two factors; MFA: two or more — different categories

VPN

An encrypted tunnel on a network you don't trust

Remote Wipe

Remotely erasing contents after a loss

Your settings don't protect you — your habits do.

Three layers you know, a passphrase you remember, five layers on your device.

Unit 9 finished · All seven domains complete

You have mastered every domain — so how do you walk into the exam room and leave having passed?

Unit 10 · Exam Strategy and Preparation