

UNIT 9 • SESSION 10

Cybersecurity

Almost nothing that goes wrong online is a technical break-in. Almost everything that goes wrong is somebody being convinced to help.

2ND SEMESTER • SCHOOL YEAR 2026-2027

Introduction to Computing • Prof. Ryan V. Labrador

Saturday, 17 October 2026 • 2-hour lecture

Two hours, five parts



Part 1

What we are protecting

Three properties. Every security decision serves one of them.



Part 2

Malware

Virus, worm, trojan, ransomware, spyware, adware — and how it really gets in



Part 3

People, not machines

Phishing, smishing, vishing, and the scams running here now



Part 4

Defending yourself

Passwords, MFA, public Wi-Fi, updates. What actually works.



Part 5

The law

Republic Act 10175, and where to report something



After

Laboratory

Phishing forensics, and a security page for your own family

By the end of today you will be able to...

1

Explain confidentiality, integrity and availability with a real example of each.

2

Tell a virus, a worm, a trojan and ransomware apart by how they spread.

3

Identify the tells in a phishing, smishing or vishing message.

4

Explain why length beats complexity in a password, with the arithmetic.

5

State the real risks of public Wi-Fi — and which old warnings no longer apply.

6

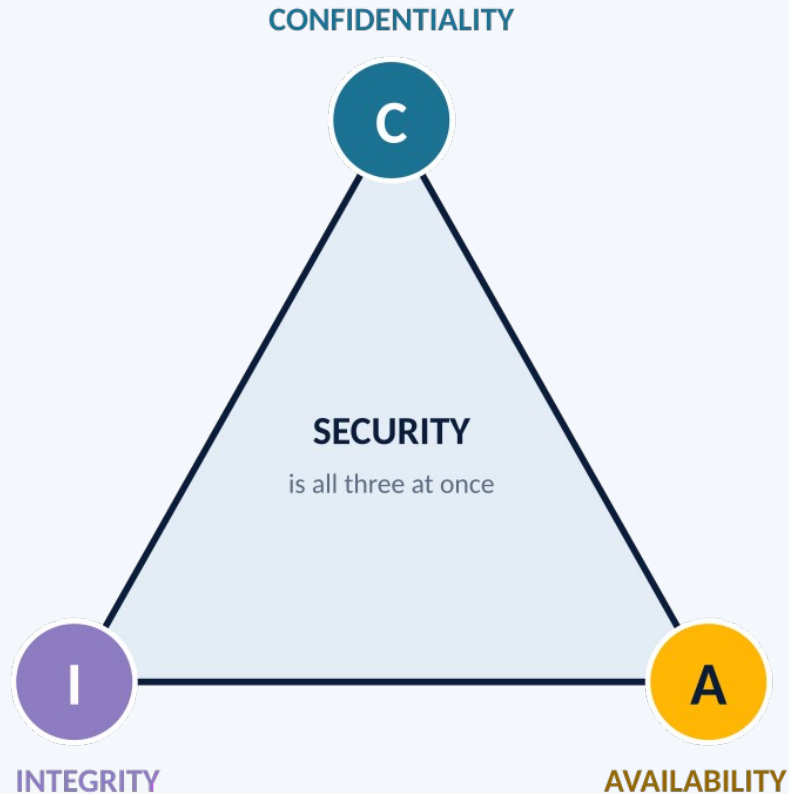
Say what RA 10175 covers and where in the Philippines to report a cybercrime.

PART 1

What are we protecting?

Before any tool, any password and any law: three properties. Everything else in this session serves one of them.

Three things worth protecting



CONFIDENTIALITY

only the people who should see it, see it

broken by: a leaked database, a reused password, a screen left facing a corridor

INTEGRITY

the data is correct and has not been altered

broken by: a changed grade, an edited balance, a quietly modified signed document

AVAILABILITY

it works at the moment you actually need it

broken by: ransomware, a flooded server room, a cut fibre, a forgotten admin password

Security is always a trade-off between these three.

Every control you meet today — a password, a backup, a locked door, an update — defends one corner of this triangle.

Confidentiality, integrity, availability



Confidentiality

Only the people who should see it, see it. Broken when medical records leak, when a password is reused, when a screen is left facing a corridor.



Integrity

The data is correct and has not been altered. Broken when a grade is changed, a balance is edited, a signed document is quietly modified.



Availability

It works when you need it. Broken by ransomware, by a flooded server room, by a cut fibre — and by a forgotten password on the only account that can fix it.

The three pull against each other. The safest system is switched off, in a locked room, and useless to everybody.

Threat, vulnerability, risk, control



Threat

Something that could harm you

A scammer, a flood, a virus, a careless colleague. It exists whether or not you are exposed.



Vulnerability

A weakness they could use

A reused password, an unpatched machine, an unlocked door, an untrained staff member.



Risk

The chance and the damage

Threat plus vulnerability plus what it would actually cost you. This is what you manage.



Control

What you do about it

MFA, backups, training, a lock. Each control reduces one specific risk — never all of them.

You cannot remove threats. You can remove vulnerabilities. That is the entire job.

PART 2

Malware

Software written to work against the person using the machine. The categories are named after how they spread, not what they do.

How it spreads



Virus

Attaches itself to a file or program. It needs a person to run that file. It cannot travel on its own — you carry it, usually on a USB stick.



Worm

Spreads by itself across a network, with nobody doing anything. This is why worms move so fast and why one unpatched machine matters to everybody.



Trojan

Pretends to be something you want. A cracked installer, a free game, a 'driver update'. You invite it in, which is exactly the design.

Virus needs you. Worm does not. Trojan tricks you. Those three sentences are the whole distinction.

What it does once it is in



Ransomware

Encrypts your files and demands payment. It attacks availability directly. Backups are the only reliable answer — and they must be offline.



Spyware

Watches. Keystrokes, screens, messages, location. It wants confidentiality, and it is designed to be boring enough that you never notice it.



Adware

Floods you with advertising and tracks you to target it. Often bundled with something free, and often the first sign that a machine has other problems too.

Ransomware attacks availability. Spyware attacks confidentiality. The triad from ten minutes ago is already doing work.

How it actually gets onto a machine

THE WAY IN	HOW COMMON	WHAT STOPS IT
Somebody ran an attachment or installer	Very common	Not opening it. Nothing else works as well.
Pirated software and cracks	Very common here	Free and legal alternatives. There are good ones.
A shared USB stick	Common	Scanning it. Not enabling autorun.
An unpatched system or browser	Common	Updates. The boring answer is the right one.
A reused password from another breach	Very common	A different password everywhere. MFA.
A genuine technical break-in	Rare	This is not how most people get hurt.

Read the last row again. The film version of hacking is the rarest row on this slide.

PART 3

People, not machines

It is far easier to convince somebody to hand over a password than to break one.
That is not a fact about technology. It is a fact about people.

Six things every scam pulls on



Urgency

Act now. Your account closes today. The offer expires in one hour. Urgency stops you checking, which is its only purpose.



Authority

I am from the bank. This is from the Dean. Uniforms, logos and job titles all work, and none of them are hard to copy.



Fear

Your account is compromised. There is a case filed against you. Frightened people comply first and think afterwards.



Greed or need

You have won. Easy money, work from home. It pulls hardest on people who genuinely need the money.



Trust

The message comes from a friend's account — because that account was taken first. The name you trust is doing the work.



Helpfulness

Somebody needs a small favour. Filipino courtesy is real, it is good, and it is routinely used as an attack surface.

Notice that none of the six is technical. Every one of them is aimed at a person, not a computer.

Phishing, smishing, vishing



Phishing

Email

A message pretending to be someone you trust, wanting a click, a login or an attachment opened.



Smishing

SMS and chat

The same, by text or Messenger. Short, urgent, and the dominant form in the Philippines.



Vishing

Voice call

A phone call. 'This is your bank's fraud team.' Hardest to resist, because a human being is waiting.



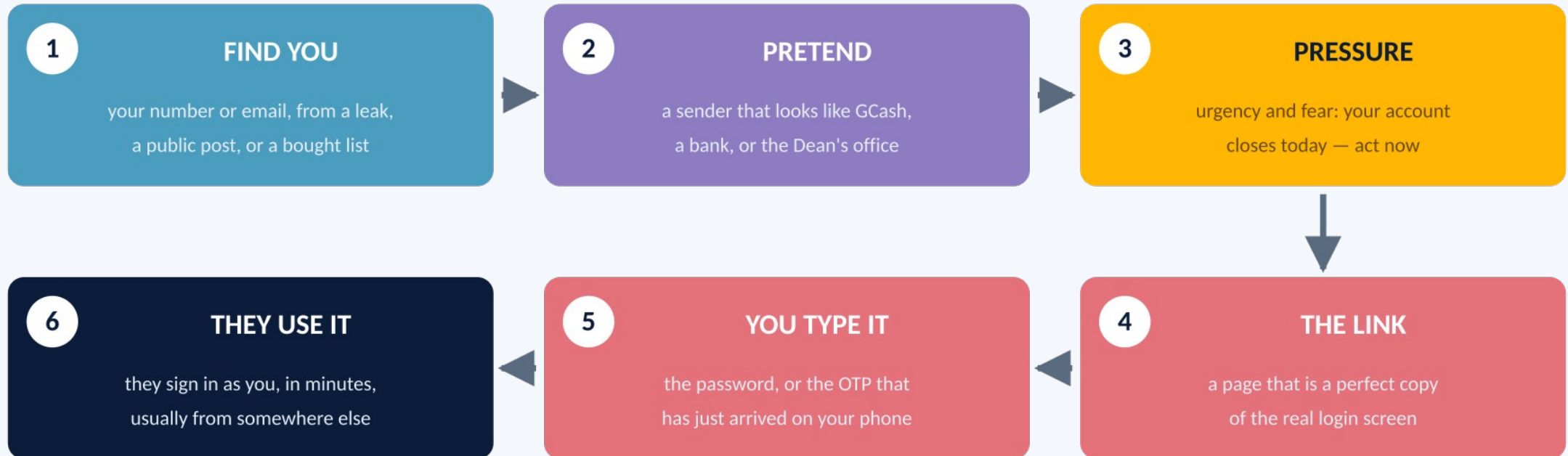
Spear phishing

Aimed at you

Uses your real name, employer, or something you posted last week. Far more convincing, and far more effective.

In this country the text message and the chat message are the main channels. Email phishing is the version in the textbook.

How a phishing attack actually runs



Not one of these six steps is technical. Every single one of them is aimed at a person.

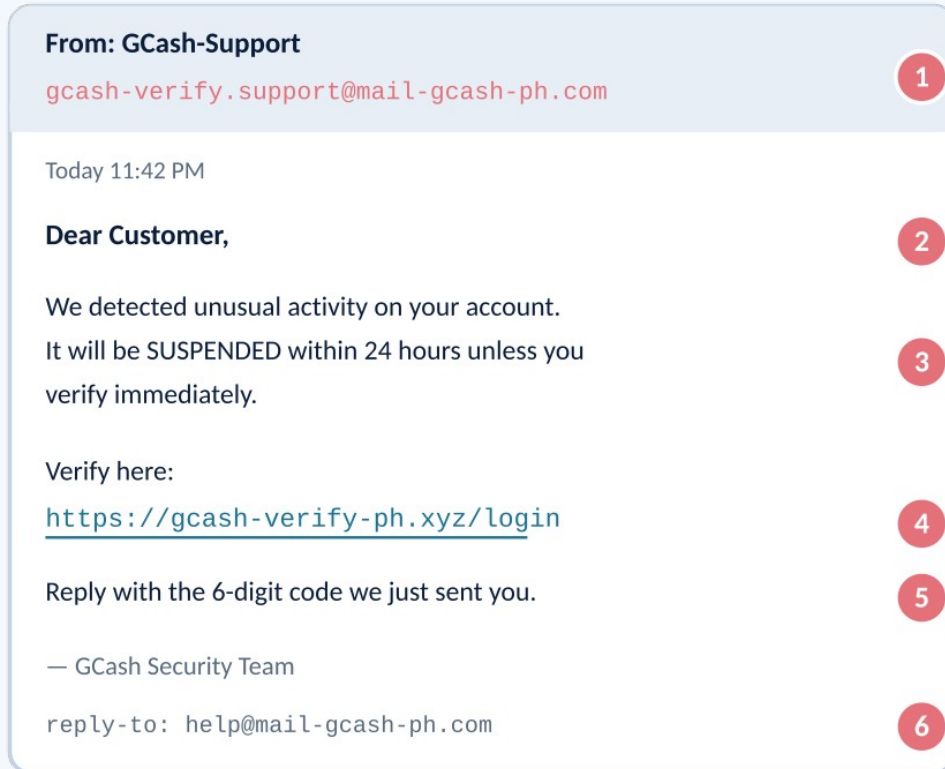
The only step you control is step 4. Everything before it has already happened without you.

The tells — what to look at, in order

LOOK AT	WHAT IS WRONG	WHY IT HAPPENS
The sender	A lookalike domain, or a personal address	They cannot use the real domain, so they use one that reads like it.
The link	Text says one thing, the link goes elsewhere	Hover, or long-press on a phone, and read the real address.
The greeting	'Dear Customer', or your email address	They are sending thousands. They do not know your name.
The urgency	A deadline, a threat, an account closing	Deliberate. It is there to stop you checking.
The request	An OTP, a PIN, a password, a fee first	This is the whole point of the message.
The channel	A reply-to that is not the institution	Your answer must reach them, not the bank.

One rule beats all six: verify on a channel YOU chose. Type the address yourself. Ring the number on the back of the card.

One message, six tells



a defanged specimen — every address here is invented and nothing is live

- 1 THE SENDER**
mail-gcash-ph.com is not gcash.com. A lookalike domain.
- 2 THE GREETING**
“Dear Customer”. They do not know your name.
- 3 THE URGENCY**
A deadline and a threat, put there to stop you checking.
- 4 THE LINK**
It says GCash. The real address ends in .xyz.
- 5 THE REQUEST**
Nobody legitimate ever asks for your OTP. Nobody.
- 6 THE CHANNEL**
The reply goes to them, not to GCash.

One rule beats all six: verify on a channel YOU chose.

This is the core skill of the session. If you can do this on a phone screen in ten seconds, you will not be caught.

Scams your family will recognise

THE APPROACH	HOW IT WORKS	THE TELL
'Wrong send' on GCash	Money arrives 'by mistake'; they ask you to send it back	You are moving stolen money. Report it; do not send.
The OTP call	'We detected suspicious activity — read me the code'	Nobody legitimate ever asks for an OTP.
Fake job offer	High pay, no interview, but a fee for training or uniform	Real employers do not charge you to be hired.
'Receive money for us'	Use your account, keep a commission	That is money laundering, and it is a crime.
Raffle or promo win	You won — pay a processing fee to release it	You cannot win a raffle you never entered.
'Ma, bagong number ko'	A relative in trouble, needing money urgently	Ring the old number. Ask something only they know.

Two rules cover most of it: nobody legitimate asks for your OTP, and money you did not expect is never a gift.

What to do, in this order



1

Stop and disconnect

Do not send anything else. Do not reply. If a device is involved, take it off the network.



2

Change the password

From a different, clean device. Change it anywhere else you used the same one — which is the real damage.



3

Tell the provider

The bank, GCash, the platform. Immediately. Speed matters more than completeness here.



4

Keep the evidence

Screenshots, numbers, reference codes, times. Do not delete the message — it is the case.



5

Report it

PNP Anti-Cybercrime Group, the NBI Cybercrime Division, or your local police station.

Step 4 is the one everybody gets wrong. Embarrassment makes people delete the evidence, and then nothing can be done.

PART 4

Defending yourself

Five things. They are unglamorous, they are free, and together they stop the overwhelming majority of what will ever be aimed at you.

Why length beats complexity



8

characters

every symbol allowed



16

characters

lowercase letters only



7 million

times more

combinations



0

reuse

the rule that matters most

The arithmetic

Length wins, badly

Eight characters from 95 symbols is a huge number. Sixteen lowercase letters is a far bigger one.

The reason

Length multiplies

Each extra character multiplies the possibilities. Swapping a for @ merely adds one guess to a list attackers already have.

Passphrases and password managers

A passphrase

- Four or five unrelated words, run together.
- Long, memorable, and quick to type on a phone.
- Must be RANDOM words — not a song lyric or a proverb.
- One good one for the manager. The rest go in it.
- Modern guidance dropped forced monthly changes.

A password manager

- Generates and stores a different password per site.
- You remember one passphrase; it remembers the rest.
- It will not fill a login box on a lookalike domain.
- That last point catches phishing automatically.
- Free options exist. Cost is not the obstacle.

Reusing one password across sites is the single most damaging habit on this slide. One breach anywhere becomes a breach everywhere.

Not all second factors are equal



SOMETHING YOU KNOW
a password or a passphrase



SOMETHING YOU HAVE
a code from an app, or a security key



SOMETHING YOU ARE
a fingerprint, or your face

FACTOR	WHAT IT IS	HOW STRONG	WEAKNESS
Password alone	Something you know	Weakest	Guessed, reused, phished, or leaked in a breach
SMS one-time code	Something you have — sort of	Better than nothing	SIM swap, and people can be talked into reading it out
Authenticator app	A code generated on your device	Good	Lose the phone without backup codes and you are locked out
Security key or passkey	A physical or built-in credential	Strongest	Costs money, or needs a supported device

Turn on any second factor today. SMS codes are the weakest kind and they are still enormously better than nothing.

The honest version

Largely solved

- 'Someone reads your password off the air.'
- Nearly every site now uses HTTPS.
- Traffic is encrypted between you and the site.
- The old warning is repeated long after it aged out.
- Repeating dead warnings makes people ignore live ones.

Still real

- An evil twin: a network with the same name, run by someone else.
- A fake sign-in page pretending to be the portal.
- 'Install this to continue.' Never. Not once.
- Apps that are not careful about encryption.
- You cannot see who is running the network.

Use it freely for ordinary things. Do not type a password into anything the NETWORK asked you to open, and never install what it offers.

What actually protects you



Update everything

Phone, PC, browser. Most malware uses a hole that was already fixed, in an update somebody postponed.



Back up, offline

Two copies, one of them not connected. This is the only real answer to ransomware and it costs almost nothing.



Least privilege

Do not run as administrator all day. Give apps only the permissions they need — check what has your camera and location.

None of this is clever. Nearly all real-world damage is prevented by things nobody finds interesting.

PART 5

The law

Republic Act 10175, the Cybercrime Prevention Act of 2012. What it covers, and where to take a case.

The Cybercrime Prevention Act of 2012

CATEGORY	WHAT IT COVERS	EVERYDAY EXAMPLE
Against systems and data	Illegal access, illegal interception, data and system interference, misuse of devices, cyber-squatting	Logging into somebody's account without permission
Computer-related offences	Computer-related forgery, computer-related fraud, computer-related identity theft	Using someone's identity to open an account
Content-related offences	Cybersex, child sexual abuse material, and libel committed online	Posting a defamatory statement about a person
Related liability	Aiding or abetting, and attempting, a cybercrime	Helping somebody carry one out
Existing crimes, done online	Crimes already in the Revised Penal Code, committed through ICT	Estafa carried out over a chat app

The Act sets penalties for each offence, and provides a higher penalty when an existing crime is committed through ICT. We are learning the categories, not memorising sentences.

The Act has limits, and there is somewhere to report

The courts

Parts were struck down

In 2014 the Supreme Court reviewed the Act and struck down several provisions as unconstitutional. A law can be passed and then narrowed.

Online libel

Narrowed by that ruling

It survived, but the Court limited who can be held liable — broadly, the original author rather than everyone who reacted or shared.

Other laws apply too

Not just RA 10175

Access device fraud, SIM registration and financial account scam laws all reach online crime. RA 10173 on data privacy is next Saturday.

Where to report

Three routes

PNP Anti-Cybercrime Group. NBI Cybercrime Division. The DOJ Office of Cybercrime. Any police station can take the initial report.

A law being on the books is not the same as a law being enforceable everywhere. Read what the courts did to it as well.

Six things from today



One

C, I and A

Every security decision protects confidentiality, integrity or availability. Usually at the cost of another.



Two

Classified by spread

Virus needs you. Worm does not. Trojan tricks you into inviting it.



Three

People, not machines

Almost nothing is broken into. Almost everything is handed over.



Four

Nobody asks for your OTP

Nobody legitimate. Not the bank, not GCash, not the platform. Ever.



Five

Length beats complexity

And reusing one password everywhere is worse than any weak password.



Six

Verify on your own channel

Type the address yourself. Ring the number you already had. Every time.

In the laboratory today



Forensics

Real, defanged specimens

Your group dissects genuine scam messages with every link disabled. Analysis only.



Score it

The tell sheet

Six things to check, in order. You mark each specimen in pen and defend your reasoning.



Build

/checker

A password strength scorer on your own rules, and those same six tells counted in code.



Compare

Your count against its count

Where the program and your own judgement disagree, the human is right. Work out why.



AI task

Red-team it

Ask an AI to judge a message, then hand it one it gets wrong. Would you let it decide for your family?

We take messages apart to learn to recognise them. Nothing is written, sent, or made usable. That rule is absolute.

PROGRAMMING LAB ACTIVITY

This afternoon

Rules a machine can check

What you are building today



Together

The group page

A /checker page: a password strength scorer on your group's own rules, and a phishing red-flag count over the three messages you caught this morning.



On your own

Your own version — this is the marked one

Your own scorer, with three rules of your own — at least one the group's page does not have — and your own four verdicts.



To match

Your page.html twin

The same thing again, typed out by hand as HTML.

WHERE IT GOES LIVE

`gNN.cic.rmlsystems.net/checker`

`gNN.cic.rmlsystems.net/<yourfolder>/`

`gNN.cic.rmlsystems.net/<yourfolder>/
page.html`

Eight identical pages is eight zeros. Your version has to be yours — your data, your words.

The Python you have not used before

if score >= 3:

do this only when it is true

elif score >= 2:

otherwise, try this one

and · or · not

join two tests into one

text.lower()

so that "URGENT" and "urgent" both match

at the shell

```
password = "ilagan2026"  
score = 0
```

```
if len(password) >= 12:  
    score += 2  
if password != password.lower():  
    score += 1
```

```
if score >= 3:  
    print("Strong enough")  
else:  
    print("Try again")
```

Made-up passwords only, today and always. Never type a real one into anything you did not write.

How this is marked

- | | | |
|---|----------------------------------|--|
| 6 | It runs | Your address loads and there is no traceback on it. |
| 6 | It does this week's thing | A real chain of conditions, in an order that gives the right answer. |
| 4 | It is yours | Three rules of your own, and one the group's page has not got. |
| 2 | The twin matches | page.html shows the same thing, by hand. |
| 2 | Worksheet complete | Including the AI sentence and the twin count. |

DUE Sunday 18 October, 11:59pm · the full guide is at labs.cic.rmlsystems.net/guides/

Nobody in your family will read a textbook.

They will read one page, written in words they use, by somebody they trust. This afternoon you write that page and put it on the internet under your own group's name. It may be the most useful thing you publish all semester.

Questions?