TRUSTED
DATA AND TECHNOLOGY
INSTITUTE

Cybersecurity Fundamentals 101

Course guide

A free course for people who work in public agencies

6 modules · 23 short video segments · about 54 minutes of video
A short quiz after Modules 1 to 5, a 12-question final quiz, and a certificate

Trusted Data and Technology Institute (TDTI)
A nonprofit public benefit corporation
info@trusteddti.com

Course guide v1 · October 16, 2026 · © 2026 Trusted Data and Technology Institute. All rights reserved.

About the course

Cybersecurity Fundamentals 101 is a free, self-paced video course from the Trusted Data and Technology Institute (TDTI). It teaches public employees the everyday habits that protect their agency and the people they serve: why agencies are targets, how to spot phishing and scams, how to keep accounts and devices safe, how to handle sensitive information, and how to report a problem fast.

Who it is for

People who work in any public agency: city, county and state offices, schools, courts, health and social services, libraries and more. No technical background is needed. The course says "the people you serve" rather than assuming one kind of agency, and every example names its setting. Each agency's own policies and procedures come first.

At a glance

Cost	Free for staff of approved public agencies
Format	Narrated video with slides and captions. Six modules of short segments, watched at your own pace.
Length	About 54 minutes of video, plus quizzes. Modules 1 to 5 run 9:38 to 10:59, and Module 6 runs 2:54. Segments run about 1 to 3 minutes.
Assessment	A 5-question quiz after each of Modules 1 to 5 (4 of 5 to pass), and a 12-question final quiz in Module 6 (10 of 12 to pass). Each module quiz has a separate retake set.
Completion	Pass the final quiz to receive a TDTI certificate showing your name, dates and the course version, then take a short course survey.

What you will be able to do

By the end of the course you will be able to:

- Explain why public agencies are targets, and why your everyday habits are the first defense
- Spot phishing by email, text, phone and QR code, and check a request another way before acting
- Stop payment fraud by verifying any change in payment details with a number you already have
- Use long, unique passwords and multifactor authentication, and never approve a prompt you didn't start
- Keep devices updated and locked, and send, store and dispose of information the approved way
- Recognize an incident, including an honest mistake, and report it fast: what, where and when
- Start three security habits this week

How your agency gets access

Step	What happens
1	Your department head, or another leader who can approve staff training, requests the training through the online form on the TDTI website or by email to **info@trusteddti.com**.
2	TDTI reviews and approves the request. The training is free for your staff.
3	Staff enroll with their agency email.
4	Staff learn at their own pace and take the final quiz.

Setup is easy and takes a few minutes. A short introduction video (1:24) walks through these steps.

Course map

Modules 1 to 5 each have three short lessons and a review segment. The review segment goes over three questions with their answers, and the module quiz follows the video. Module 6 ends with the final quiz.

#	Title	Segments	Video	Assessment
1	**Why security is part of your job**	Why attackers target public agencies, What attackers want, Four habits that protect you, review	10:59	5-question quiz (4 of 5)
2	**Phishing and scams**	Spotting a phishing email, Texts, calls, QR codes and fake voices, Payment and invoice fraud, review	10:40	5-question quiz (4 of 5)
3	**Passwords and sign-in safety**	Strong passwords, Multifactor authentication, Keeping your account yours, review	10:22	5-question quiz (4 of 5)
4	**Protecting devices and information**	Updates and locked screens, Working safely in and out of the office, Handling sensitive information, review	9:42	5-question quiz (4 of 5)
5	**Spot it, report it**	What an incident looks like, I clicked. Now what?, How and what to report, review	9:38	5-question quiz (4 of 5)
6	**Action plan and final quiz**	Your security checklist, Course recap, Final quiz and what's next	2:54	12-question final quiz (10 of 12)
	Course introduction	What the course covers and how your agency gets access	1:24	None
	Total		**0:54:16**	

Video lengths are measured from the current course videos and include the title cards between segments. The total does not include the introduction video or time spent on quizzes.

MODULE 1

Why security is part of your job

10:59 of video · four segments · 5-question quiz after the video

Learners see why public agencies are targets, what attackers want, how many attacks begin with a person, and the four everyday habits that stop many attacks.

What you will learn

- Why public agencies are targets
- What an attack can cost
- Why your habits matter

Segments

#	Segment	Length
1.1	**Why attackers target public agencies** Who the course is for, why public agencies are targets, and what an attack can cost. **Key points:** Agencies hold information, money and services people need · That makes every employee a possible target	2:56
1.2	**What attackers want** Information, money and access; keeping information private, correct and running; how many attacks begin. **Key points:** Attackers want information, money and access · Many attacks start with a person, not a machine	2:26
1.3	**Four habits that protect you** CISA's four habits, where the course covers each one, and why your agency's rules come first. **Key points:** Report phishing, strong passwords, MFA, updates · Your agency's rules come first	2:19
1.4	**Review and knowledge check** Three review questions with answers, then the module quiz.	3:09

MODULE 2

Phishing and scams

10:40 of video · four segments · 5-question quiz after the video

Learners spot the warning signs of phishing by email, text, phone and QR code, check a familiar voice another way, and stop payment and invoice fraud by verifying with a number they already have.

What you will learn

- What phishing is
- Four warning signs
- What to do instead of clicking

Segments

#	Segment	Length
2.1	**Spotting a phishing email** What phishing is, four warning signs in a sample county HR email, and what to do instead of clicking. **Key points:** Pause before you click · Check another way, then report it	2:28
2.2	**Texts, calls, QR codes and fake voices** Phishing by text and phone, fake QR codes, and AI voices that pose as officials (FBI warning, May 2025). **Key points:** Texts, calls and QR codes can be phishing too · Hang up, then call back on a known number	2:30
2.3	**Payment and invoice fraud** Business email compromise, a request to change a vendor's bank account, and verifying before you pay. **Key points:** Any change in payment details is a warning sign · Verify by calling a number you already have	2:24
2.4	**Review and knowledge check** Three review questions with answers, then the module quiz.	3:08

MODULE 3

Passwords and sign-in safety

10:22 of video · four segments · 5-question quiz after the video

Learners make long, unique passwords with help from an approved password manager, turn on multifactor authentication, never approve a prompt they didn't start, and act fast if an account looks compromised.

What you will learn

- Why length matters most
- One password for each account
- Let a password manager help

Segments

#	Segment	Length
3.1	**Strong passwords** Why length beats complexity, one password for each account, and letting a password manager help. **Key points:** Long, unique and never reused · Use your agency's approved password manager	2:23
3.2	**Multifactor authentication** What multifactor authentication is, common kinds, and never approving a prompt you didn't start. **Key points:** Turn on MFA wherever you can · Never approve a prompt you didn't start	2:23
3.3	**Keeping your account yours** Never sharing your login, signs that someone else is in your account, and what to do if a password leaks. **Key points:** Your login is yours alone · Act fast when something looks wrong	2:20
3.4	**Review and knowledge check** Three review questions with answers, then the module quiz.	3:07

MODULE 4

Protecting devices and information

9:42 of video · four segments · 5-question quiz after the video

Learners keep devices updated and locked, work safely in the field and around the office, and send, store and dispose of sensitive information the approved way.

What you will learn

- Why updates matter
- Lock your screen every time
- Use only approved software

Segments

#	Segment	Length
4.1	**Updates and locked screens** Installing updates, locking your screen every time, and using only approved software. **Key points:** Update it, lock it, and use approved software	2:03
4.2	**Working safely in and out of the office** Working away from the office, unknown USB drives, and secure doors, badges and printouts. **Key points:** Approved connections, devices kept close · Unknown drives go to IT	2:09
4.3	**Handling sensitive information** Four levels of information, sending it the approved way, and storing and disposing of it safely. **Key points:** Know the level, and send it the approved way · Store it safely, and dispose of it properly	2:17
4.4	**Review and knowledge check** Three review questions with answers, then the module quiz.	3:04

MODULE 5

Spot it, report it

9:38 of video · four segments · 5-question quiz after the video

Learners recognize an incident, including honest mistakes, take the right first steps after a bad click, and report what happened, where and when.

What you will learn

- What counts as an incident
- Signs on your computer or account
- Why mistakes count too

Segments

#	Segment	Length
5.1	**What an incident looks like** What counts as an incident, signs on your computer or account, and why honest mistakes count too. **Key points:** Attacks and mistakes are both incidents · When in doubt, treat it as one	2:09
5.2	**I clicked. Now what?** The first steps after a bad click, a courthouse example of a quick report, and why speed matters. **Key points:** Stop, don't hide it, report it fast	2:15
5.3	**How and what to report** Who to tell, what to include in a report, and how reporting protects the people you serve. **Key points:** Know who to tell before you need to · What, where and when	2:08
5.4	**Review and knowledge check** Three review questions with answers, then the module quiz.	2:57

MODULE 6

Action plan and final quiz

2:54 of video · three segments · 12-question final quiz

Learners pick three security habits to start this week, review the whole course, and take the 12-question final quiz for the certificate.

What you will do

- Pick three security habits to start this week
- Review the main idea of each module
- Take the final quiz and receive your certificate

Segments

#	Segment	Length
6.1	**Your security checklist** Picking three habits for this week, with a school district office manager's plan as an example. **Key points:** Small habits, every day	1:15
6.2	**Course recap** The whole course in five lines.	0:33
6.3	**Final quiz and what's next** How the final quiz and certificate work, and a thank-you.	1:00

Quizzes and certificate

Module quizzes (Modules 1 to 5)

- Each module ends with three review questions in the video. Each question is shown, read aloud and answered, using true or false or four choices.
- After the video comes a 5-question quiz on the module, with new questions. Score 4 of 5 (80%) to move on.
- If you do not pass, review the module and take the retake set, a separate group of five questions.

Final quiz (Module 6)

- 12 new questions drawn from Modules 1 to 5.
- Score 10 of 12 to pass. 9 of 12 is 75% and does not pass.
- Not yet? Review and try again.

Certificate

- Pass the final quiz to receive your TDTI certificate.
- It shows your name, your dates and the course version.
- Then take the short course survey.

Your security habits

In Module 6 you write down three habits to start this week, such as turning on multifactor authentication, reporting the next suspicious message the right way, and saving your help desk number in your phone. Keep the list, and follow your agency's own policies and procedures.

Sources

The course content is checked against the published sources below. Each slide in the course files lists the sources it relies on, and the course files hold the exact passages quoted. Access dates are in October 2026.

Source	Used in
FBI Internet Crime Complaint Center, 2024 Internet Crime Report (released April 2025) https://www.aha.org/cybersecurity-government-intelligence-reports/2025-05-12-2024-fbi-internet-crime-report):	M1, M2, M5
CISA, 'Require Multifactor Authentication' (accessed 2026-10-16) https://www.cisa.gov/require-multifactor-authentication	M1, M3
CISA, Secure Our World videos (accessed 2026-10-16) https://www.cisa.gov/secure-our-world-videos	M1, M6
CISA, Secure Our World, 'Update Software' (accessed 2026-10-16) https://www.cisa.gov/secure-our-world/update-software	M1, M4
CISA, Secure Our World, 'Recognize and Report Phishing' (accessed 2026-10-16) https://www.cisa.gov/secure-our-world/recognize-and-report-phishing	M2, M5
FBI IC3 Public Service Announcement I-051525-PSA, 'Senior US Officials Impersonated in Malicious Messaging Campaign' (May 15, 2025; accessed 2026-10-16) https://www.ic3.gov/PSA/2025/PSA250515	M2
CISA Secure Our World tip sheet 'Avoid Phishing Scams with Three Simple Tips' (copy hosted by Mass.gov, 2023; accessed 2026-10-16) https://www.mass.gov/files/documents/2023/10/12/Secure-Our-World-Phishing-Tip-Sheet.pdf	M2
NIST SP 800-63B-4, Digital Identity Guidelines: Authentication and Authenticator Management (final published July 31, 2025, per) https://csrc.nist.gov/pubs/sp/800/63/b/4/final	M3
CISA, guidance on phishing-resistant and number-matching MFA (October 31, 2022), as summarized by Health-ISAC (November 1, 2022) https://www.aha.org/system/files/media/file/2022/11/cisa-tlp-white-guidance-on-phishing-resistant-and-numbers-matching-multifactor-authentication-11-1-22.pdf	M3
CISA, 'More than a Password' (accessed 2026-10-16) https://www.cisa.gov/MFA	M3
CISA Secure Our World passwords tip sheet (copy hosted by Mass.gov, 2023; accessed 2026-10-16) https://www.mass.gov/files/documents/2023/10/06/Secure-Our-World-Passwords-Tip-Sheet.pdf	M3

Course policies (pass marks, the access process, the audience wording and the action plan design) were set by TDTI and are recorded in the course outline (v0.2, October 16, 2026). Examples in the course are invented.