CYBERSECURITY TIP SHEET

RED FLAGS, COMMON MISTAKES, FAST FIXES

Version 2025-12-31

αPlan

ID	SECTION	TOPIC	KEY TAKEAWAYS	KEY TERMS	RED FLAG / COMMON MISTAKE	DO THIS (BEST PRACTICE)	IF UNSURE / REPORT	IMPACT	LIKELIHOOD	PRIORITY SCORE	SRC
1	**Cybersecurity 101**	Why cybersecurity matters	Security protects confidentiality, integrity, and availability (CIA) of business data and systems.	CIA triad, risk, threat	Thinking 'IT handles security' so I don't need to act.	Treat security as part of your job; follow policy, report incidents quickly.	Report suspicious activity to your security/IT helpdesk immediately.	4	3	12 Medium	1
2	**Cybersecurity 101**	Attack chain basics	Most incidents follow steps such as recon, initial access, execution, persistence, and impact. Early reporting breaks the chain.	initial access, malware, persistence	Ignoring 'small' anomalies like unexpected MFA prompts.	Report anomalies early; don't wait for proof.	If you receive unexpected MFA prompts, report and change your password.	5	3	15 High	2
3	**Cybersecurity 101**	Passwords vs MFA	Strong unique passwords plus MFA reduce account takeover risk.	MFA, password manager, credential stuffing	Reusing passwords across sites.	Use a password manager; enable MFA everywhere it's offered.	If you suspect password reuse, change passwords starting with email and SSO.	5	4	20 Critical	3
4	**Cybersecurity 101**	Updates and patching	Timely updates close known vulnerabilities exploited by attackers.	patching, vulnerability, CVE	Clicking 'remind me later' indefinitely.	Install updates promptly; reboot when required.	If an update prompt looks suspicious, verify via official app store/IT channel.	4	3	12 Medium	1
5	**Cybersecurity 101**	Backups (what you can do)	Backups enable recovery from ransomware or accidental deletion.	backup, ransomware, recovery	Storing the only copy of critical files on a local device.	Save work in approved, backed-up systems (e.g., corporate cloud drives).	If files disappear or look encrypted, disconnect and report immediately.	5	3	15 High	2
6	**InfoSec Terminology**	Authentication vs authorization	Authentication proves who you are; authorization defines what you can do.	authN, authZ, IAM	Assuming login access implies permission to share data.	Verify access rights before sharing; apply least privilege.	If unsure, ask the data owner or IT for correct access.	4	3	12 Medium	1
7	**InfoSec Terminology**	Least privilege	Grant the minimum access needed for the job and remove unused access.	least privilege, RBAC	Keeping admin rights 'just in case'.	Request temporary elevated access only when needed; review access regularly.	If you see access you don't need, request removal.	4	3	12 Medium	2
8	**InfoSec Terminology**	Data classification	Handle data according to its sensitivity (e.g., public, internal, confidential).	data classification, PII	Sending confidential data over personal email or consumer chat tools.	Use approved tools and labels; share only with authorized recipients.	If you mis-send data, report immediately, because speed matters.	5	3	15 High	1
9	**InfoSec Terminology**	Encryption vs hashing	Encryption is reversible with a key; hashing is one-way for integrity checks.	encryption, hashing, key	Assuming 'hashed' means 'encrypted'.	Use approved encryption for data at rest/in transit; protect keys.	If asked to store secrets, use a secrets manager, not documents.	4	2	8 Low	1
10	**InfoSec Terminology**	Logs and monitoring	Logs provide evidence for detection, response, and auditing.	logs, telemetry, SIEM	Disabling security tools because they seem 'noisy'.	Do not disable security tools; report issues to IT/security.	If you suspect compromise, preserve evidence; don't wipe devices.	5	2	10 Low-Med	4
11	**AI Basics**	What AI is (plain terms)	AI systems learn patterns from data to make predictions or generate content; outputs can be wrong.	machine learning, model, inference	Treating AI output as guaranteed fact.	Verify AI outputs, especially numbers, quotes, and instructions.	If output is high-stakes, use authoritative sources or human review.	4	3	12 Medium	5
12	**AI Basics**	LLMs and hallucinations	LLMs predict likely text and can 'hallucinate' plausible but false answers.	LLM, hallucination	Using AI-generated instructions in production without review.	Cross-check against trusted docs; test in safe environments.	If uncertain, consult an SME or official vendor documentation.	4	3	12 Medium	6
13	**AI Basics**	Prompting safely	Prompts can expose sensitive info; assume prompts may be logged.	prompt, data leakage	Pasting customer data, secrets, or passwords into AI tools.	Use approved AI tools; redact sensitive data; follow policy.	If you shared sensitive data accidentally, report per policy.	5	3	15 High	5
14	**AI Basics**	Training vs inference	Training builds the model; inference is using it, and the risks differ for each.	training, inference, fine-tuning	Uploading proprietary datasets to unapproved tools.	Use approved environments for model work; document data sources.	If data provenance is unclear, stop and escalate.	4	2	8 Low	6
15	**AI Basics**	Model inputs as attack surface	AI systems can be manipulated via crafted inputs (e.g., prompt injection).	prompt injection, adversarial input	Blindly following AI-suggested links or commands.	Treat AI output like untrusted input; validate before acting.	If AI gives unexpected system-level instructions, stop and report.	5	2	10 Low-Med	6
16	**AI in Cybersecurity**	AI as a defender (what it helps)	AI can assist with alert triage, anomaly detection, and summarization, all under human oversight.	SOAR, SIEM, anomaly detection	Assuming AI detection is 'set and forget'.	Use AI to augment analysts; keep tuning, validation, and audit trails.	If AI decisions affect customers, require human review gates.	4	2	8 Low	5
17	**AI in Cybersecurity**	AI as a target	Attackers may attempt data poisoning, model theft, or inference attacks against AI systems.	data poisoning, model extraction, inversion	Exposing model APIs without rate limits or monitoring.	Apply authentication, throttling, logging, and abuse monitoring to AI endpoints.	If model behavior shifts unexpectedly, investigate data/prompt changes.	5	2	10 Low-Med	6
18	**AI in Cybersecurity**	Shadow AI risk	Unapproved AI tools can leak data and bypass governance.	shadow AI, governance	Employees using personal AI accounts for work data.	Provide approved tools; train staff on permitted use; monitor egress.	If you need a capability, request an approved solution.	4	3	12 Medium	5
19	**AI in Cybersecurity**	Secure use of AI copilots	Copilots can suggest insecure code or configurations.	secure SDLC, code review	Accepting code suggestions without security review.	Use secure coding standards; run SAST/DAST; peer review.	If uncertain, consult security engineering or AppSec.	5	2	10 Low-Med	1
20	**AI in Cybersecurity**	AI and incident response	AI can speed investigation summaries, but evidence handling and decisions remain human-led.	incident response, chain of custody	Letting AI overwrite or transform original evidence.	Preserve originals; use AI on copies; document steps.	If an incident is suspected, follow IR playbooks.	5	2	10 Low-Med	4
21	**Social Engineering Basics**	What social engineering is	Manipulating people is often easier than hacking systems.	social engineering, persuasion	Requests that bypass process due to urgency.	Slow down; verify identity and authorization.	When pressured, insist on standard verification steps.	5	4	20 Critical	3
22	**Social Engineering Basics**	Phishing (email)	Phishing lures you into clicking links, opening attachments, or sharing information.	phishing, spoofing	Unexpected attachment, mismatched domain, urgent payment request.	Preview links safely; verify sender; report via your phishing reporting method.	If you clicked or opened something, report immediately and follow IT guidance.	5	4	20 Critical	7
23	**Social Engineering Basics**	Vishing & smishing	Voice and SMS phishing exploit trust and urgency.	vishing, smishing	Caller ID looks legitimate; asks for OTP or password.	Never share passwords/OTP; call back using a trusted directory number.	If you shared info, report and reset credentials immediately.	5	3	15 High	8

PRIORITY = IMPACT (1-5) x LIKELIHOOD (1-5)

- 8 Low
- 10 Low-Med
- 12 Medium
- 15 High
- 20 Critical

SOURCES

1 NIST Cybersecurity Framework
2 NIST CSF 2.0 (CSWP 29)
3 CISA - Recognize & Report Phishing
4 NIST SP 800-61r3 - Incident Response
5 NIST AI Risk Management Framework
6 NIST AI 100-1 (AI RMF)
7 CISA - Phishing Guidance
8 CISA - Avoiding Social Engineering

Full glossary, worked scenarios and a mini-quiz are in the companion workbook (Glossary, Scenarios and Mini Quiz tabs).

Disclaimer: This material was created on behalf of the 'U.S. Cybersecurity Leadership in AI for Albania' project, funded by the United States Department of State. The opinions, findings, and conclusions stated herein are those of the authors and do not necessarily reflect those of the United States Department of State.

CYBERSECURITY TIP SHEET

RED FLAGS, COMMON MISTAKES, FAST FIXES

Version 2025-12-31

αPlan

ID	SECTION	TOPIC	KEY TAKEAWAYS	KEY TERMS	RED FLAG / COMMON MISTAKE	DO THIS (BEST PRACTICE)	IF UNSURE / REPORT	IMPACT	LIKELIHOOD	PRIORITY SCORE	SRC
24	**Social Engineering Basics**	Pretexting and impersonation	Attackers may pose as IT, executives, vendors, or new employees.	pretexting, impersonation	Unusual requests for access, invoices, gift cards, or wire transfers.	Follow approval workflows; verify via secondary channel.	If someone insists on bypassing controls, escalate to manager/security.	5	3	15 High	8
25	**Social Engineering Basics**	Physical social engineering	Tailgating and shoulder surfing can bypass digital controls.	tailgating, badge, clean desk	Someone without a badge asking to be let in.	Don't badge others in; escort visitors; lock screen when away.	Report suspicious physical behavior to facilities/security.	4	2	8 Low	1
26	**Social Engineering in the Age of AI**	AI-written phishing	Generative AI can produce more convincing, personalized messages at scale.	AI phishing, spearphishing	Messages with perfect grammar but unusual requests or timing.	Verify requests through a separate, trusted channel; treat links/attachments as hostile.	If a message seems unusually tailored, report for analysis.	5	4	20 Critical	7
27	**Social Engineering in the Age of AI**	Deepfakes (video/audio)	Deepfakes can mimic executives or coworkers to request sensitive actions.	deepfake, voice cloning	A call/video with urgency; refuses call-back; unusual phrasing.	Use call-back verification and approval workflows; require written confirmation.	If suspected, preserve evidence (as policy allows) and report.	5	3	15 High	5
28	**Social Engineering in the Age of AI**	Synthetic identities	Attackers may create realistic personas using AI-generated photos and profiles.	synthetic identity, OSINT	New contact with minimal history requesting access or favors.	Verify identity via HR/vendor management; use official channels.	If unsure, do not engage; forward to security.	4	3	12 Medium	3
29	**Social Engineering in the Age of AI**	BEC + AI	AI can help attackers mimic writing style to request payments or data.	BEC, invoice fraud	Payment change requests via email only.	Confirm changes via known phone numbers; require dual approval.	If a payment was sent, contact finance and security immediately.	5	3	15 High	3
30	**Social Engineering in the Age of AI**	AI-assisted reconnaissance	Attackers can use AI to scale research on org charts and vendors.	reconnaissance, OSINT	Oversharing internal details on social media.	Limit public info; follow disclosure guidelines.	If you notice sensitive info public, request removal and alert security.	4	2	8 Low	1
31	**Cybersecurity 101**	Incident reporting	Fast reporting reduces impact; you are not expected to investigate alone.	incident, escalation	Trying to 'fix it yourself' and delaying reporting.	Report immediately with what you saw, when, and which device/app was involved.	Use official incident channels; keep notes/screenshots if safe.	5	3	15 High	4
32	**InfoSec Terminology**	PII vs sensitive data	PII identifies a person; sensitive data can include credentials, financial data, health data, and more.	PII, PHI, PCI	Sharing spreadsheets with customer data broadly.	Minimize sharing; use secure transfer; apply need-to-know.	If data handling is unclear, consult privacy/security.	5	3	15 High	1
33	**AI Basics**	Bias and fairness	AI can reflect bias in its training data; outcomes should be monitored.	bias, fairness, drift	Assuming AI decisions are 'objective'.	Test outputs for fairness; document limitations.	If decisions affect people, add human review and appeal paths.	4	2	8 Low	6
34	**AI in Cybersecurity**	Security of AI data pipelines	Data used for AI is high-value; protect provenance, access, and integrity.	data pipeline, provenance	Using unknown datasets or unmanaged storage locations.	Control access; version datasets; validate inputs; monitor changes.	If you detect tampering, stop pipeline and escalate.	5	2	10 Low-Med	6
35	**Social Engineering Basics**	Authority and urgency cues	Attackers exploit authority and urgency to short-circuit controls.	urgency, authority, reciprocity	Threats like 'account will be closed today' demanding immediate action.	Pause; verify; ask a colleague for a second look.	If you feel rushed, that is a signal to slow down.	5	4	20 Critical	8
36	**Social Engineering in the Age of AI**	Verification playbook	Use multi-step identity verification for sensitive requests, especially those received digitally.	separate channel, verification	Request arrives via chat/video asking for access or payment.	Call back using directory; require ticket/approval; confirm with manager.	If verification fails, stop and report.	5	4	20 Critical	3

PRIORITY = IMPACT (1-5) x LIKELIHOOD (1-5)

- **8** Low
- **10** Low-Med
- **12** Medium
- **15** High
- **20** Critical

SOURCES

1 NIST Cybersecurity Framework
2 NIST CSF 2.0 (CSWP 29)
3 CISA - Recognize & Report Phishing
4 NIST SP 800-61r3 - Incident Response
5 NIST AI Risk Management Framework
6 NIST AI 100-1 (AI RMF)
7 CISA - Phishing Guidance
8 CISA - Avoiding Social Engineering

Full glossary, worked scenarios and a mini-quiz are in the companion workbook (Glossary, Scenarios and Mini Quiz tabs).

Disclaimer: This material was created on behalf of the 'U.S. Cybersecurity Leadership in AI for Albania' project, funded by the United States Department of State. The opinions, findings, and conclusions stated herein are those of the authors and do not necessarily reflect those of the United States Department of State.