SECURITY ANALYZER

CYBERSECURITY AWARENESS & CORPORATE SECURITY GUIDE

LEVEL 1 - FUNDAMENTAL TRAINING FOR ALL EMPLOYEES

Complete rebuilt English edition - 2026

MISSION

Build practical security judgment across the whole organization: STOP when context changes, CHECK identity and procedure independently, REPORT suspicious events and mistakes quickly.

Introduction - Security is a shared operating discipline

This handbook is intended for every employee, contractor and manager who uses company information or systems. It assumes no specialist cybersecurity knowledge. Its purpose is to build practical judgment: recognizing when an ordinary business action has become risky, knowing how to verify it, and knowing when to stop and report.

Technical controls are indispensable, but they cannot interpret every business situation. A payment can be technically authorized and still be fraudulent. A real cloud platform can be reached through a malicious login link. A valid employee account can be controlled by an attacker. Human context therefore remains part of the security control system.

A strong security culture is not based on fear. Many incidents can be contained if the security team learns about them quickly. Employees should never delay reporting because they are embarrassed or uncertain. A near miss is valuable information because it can expose a confusing workflow, an ineffective warning or an unnecessary privilege.

THE METHOD

STOP: pause when a request is unexpected, urgent, secret or inconsistent with procedure. CHECK: verify through a channel you already trust. REPORT: escalate suspicious events and mistakes through the designated mechanism.

1. Cybersecurity as a business discipline

Learning objective: understand operations, people, information, money and trust.

Why this matters

This chapter deals with operations, people, information, money and trust. Security incidents rarely depend on one spectacular technical trick. More often, an attacker combines ordinary information, a believable pretext and one action from a legitimate user. The employee's task is not to diagnose malware or perform forensics; it is to recognize when normal context has changed and to slow the transaction down long enough to verify it.

How the attack works

Attackers usually seek one of five outcomes: credentials, an authentication approval, execution of a file or action, disclosure of information, or redirection of a legitimate business process. The request can therefore look completely normal. Compare it with the expected workflow: who normally asks, through which channel, with which approvals, and at what stage of the process?

Warning signals

Useful signals include unexpected urgency, unusual secrecy, a new communication channel, a changed domain or payment detail, a request to bypass a control, a login you did not initiate, or pressure to act before verification. None of these proves an attack by itself. Their purpose is to trigger a verification step. Good awareness is disciplined uncertainty, not panic.

Realistic situations

Discuss these situations: a supplier request that changes procedure; an unexpected login alert; an accidental external share. For each one, separate the business story from the evidence of identity. Ask whether the event was expected, whether it follows the normal process, whether the person can be confirmed using contact information already known to the organization, and what the consequence would be if you waited five minutes before acting.

Required behavior

The core practices are: know the reporting channel; verify procedural changes; report mistakes immediately. These controls must be connected to real company procedures. A policy that cannot be followed during ordinary work will eventually be bypassed, so managers must make the secure route clear and usable.

If you already made the mistake

Do not waste time trying to hide, undo or investigate the event alone. Record what happened, the approximate time, the device and service involved, and exactly what you entered, opened, approved, sent or changed. Contact the designated security channel immediately. Fast factual reporting may allow sessions to be revoked, transactions to be stopped, credentials to be reset or affected devices to be isolated.

Team exercise

Identify one normal workflow related to this chapter and one point where an attacker could imitate a legitimate request. Then identify an independent verification method. This exercise turns awareness into an operational control. The objective is not to catch employees making mistakes; it is to discover where the business process makes a dangerous action too easy.

CHAPTER CHECK

Can you name the normal procedure, an independent verification channel and the incident-reporting route for this subject? If not, resolve that gap before an incident occurs.

2. Identity and passwords

Learning objective: understand the digital identity attached to every employee account.

Why this matters

This chapter deals with the digital identity attached to every employee account. Security incidents rarely depend on one spectacular technical trick. More often, an attacker combines ordinary information, a believable pretext and one action from a legitimate user. The employee's task is not to diagnose malware or perform forensics; it is to recognize when normal context has changed and to slow the transaction down long enough to verify it.

How the attack works

Attackers usually seek one of five outcomes: credentials, an authentication approval, execution of a file or action, disclosure of information, or redirection of a legitimate business process. The request can therefore look completely normal. Compare it with the expected workflow: who normally asks, through which channel, with which approvals, and at what stage of the process?

Warning signals

Useful signals include unexpected urgency, unusual secrecy, a new communication channel, a changed domain or payment detail, a request to bypass a control, a login you did not initiate, or pressure to act before verification. None of these proves an attack by itself. Their purpose is to trigger a verification step. Good awareness is disciplined uncertainty, not panic.

Realistic situations

Discuss these situations: a reused password exposed by another website; a fake IT caller; credentials saved on a shared PC. For each one, separate the business story from the evidence of identity. Ask whether the event was expected, whether it follows the normal process, whether the person can be confirmed using contact information already known to the organization, and what the consequence would be if you waited five minutes before acting.

Required behavior

The core practices are: use unique credentials; use an approved password manager; protect recovery methods. These controls must be connected to real company procedures. A policy that cannot be followed during ordinary work will eventually be bypassed, so managers must make the secure route clear and usable.

If you already made the mistake

Do not waste time trying to hide, undo or investigate the event alone. Record what happened, the approximate time, the device and service involved, and exactly what you entered, opened, approved, sent or changed. Contact the designated security channel immediately. Fast factual reporting may allow sessions to be revoked, transactions to be stopped, credentials to be reset or affected devices to be isolated.

Team exercise

Identify one normal workflow related to this chapter and one point where an attacker could imitate a legitimate request. Then identify an independent verification method. This exercise turns awareness into an operational control. The objective is not to catch employees making mistakes; it is to discover where the business process makes a dangerous action too easy.

CHAPTER CHECK

Can you name the normal procedure, an independent verification channel and the incident-reporting route for this subject? If not, resolve that gap before an incident occurs.

3. Multi-factor authentication

Learning objective: understand the additional proof used to protect an account when a password is stolen.

Why this matters

This chapter deals with the additional proof used to protect an account when a password is stolen. Security incidents rarely depend on one spectacular technical trick. More often, an attacker combines ordinary information, a believable pretext and one action from a legitimate user. The employee's task is not to diagnose malware or perform forensics; it is to recognize when normal context has changed and to slow the transaction down long enough to verify it.

How the attack works

Attackers usually seek one of five outcomes: credentials, an authentication approval, execution of a file or action, disclosure of information, or redirection of a legitimate business process. The request can therefore look completely normal. Compare it with the expected workflow: who normally asks, through which channel, with which approvals, and at what stage of the process?

Warning signals

Useful signals include unexpected urgency, unusual secrecy, a new communication channel, a changed domain or payment detail, a request to bypass a control, a login you did not initiate, or pressure to act before verification. None of these proves an attack by itself. Their purpose is to trigger a verification step. Good awareness is disciplined uncertainty, not panic.

Realistic situations

Discuss these situations: an unexpected push notification; a caller requesting a one-time code; repeated MFA prompts. For each one, separate the business story from the evidence of identity. Ask whether the event was expected, whether it follows the normal process, whether the person can be confirmed using contact information already known to the organization, and what the consequence would be if you waited five minutes before acting.

Required behavior

The core practices are: approve only requests you initiated; never disclose codes; reject and report unexpected prompts. These controls must be connected to real company procedures. A policy that cannot be followed during ordinary work will eventually be bypassed, so managers must make the secure route clear and usable.

If you already made the mistake

Do not waste time trying to hide, undo or investigate the event alone. Record what happened, the approximate time, the device and service involved, and exactly what you entered, opened, approved, sent or changed. Contact the designated security channel immediately. Fast factual reporting may allow sessions to be revoked, transactions to be stopped, credentials to be reset or affected devices to be isolated.

Team exercise

Identify one normal workflow related to this chapter and one point where an attacker could imitate a legitimate request. Then identify an independent verification method. This exercise turns awareness into an operational control. The objective is not to catch employees making mistakes; it is to discover where the business process makes a dangerous action too easy.

CHAPTER CHECK

Can you name the normal procedure, an independent verification channel and the incident-reporting route for this subject? If not, resolve that gap before an incident occurs.

4. Email phishing and impersonation

Learning objective: understand the manipulation of email trust, identity and business context.

Why this matters

This chapter deals with the manipulation of email trust, identity and business context. Security incidents rarely depend on one spectacular technical trick. More often, an attacker combines ordinary information, a believable pretext and one action from a legitimate user. The employee's task is not to diagnose malware or perform forensics; it is to recognize when normal context has changed and to slow the transaction down long enough to verify it.

How the attack works

Attackers usually seek one of five outcomes: credentials, an authentication approval, execution of a file or action, disclosure of information, or redirection of a legitimate business process. The request can therefore look completely normal. Compare it with the expected workflow: who normally asks, through which channel, with which approvals, and at what stage of the process?

Warning signals

Useful signals include unexpected urgency, unusual secrecy, a new communication channel, a changed domain or payment detail, a request to bypass a control, a login you did not initiate, or pressure to act before verification. None of these proves an attack by itself. Their purpose is to trigger a verification step. Good awareness is disciplined uncertainty, not panic.

Realistic situations

Discuss these situations: a look-alike Microsoft login; a fake shared document; an executive gift-card request. For each one, separate the business story from the evidence of identity. Ask whether the event was expected, whether it follows the normal process, whether the person can be confirmed using contact information already known to the organization, and what the consequence would be if you waited five minutes before acting.

Required behavior

The core practices are: inspect the real sender and domain; verify unusual requests independently; report suspicious mail. These controls must be connected to real company procedures. A policy that cannot be followed during ordinary work will eventually be bypassed, so managers must make the secure route clear and usable.

If you already made the mistake

Do not waste time trying to hide, undo or investigate the event alone. Record what happened, the approximate time, the device and service involved, and exactly what you entered, opened, approved, sent or changed. Contact the designated security channel immediately. Fast factual reporting may allow sessions to be revoked, transactions to be stopped, credentials to be reset or affected devices to be isolated.

Team exercise

Identify one normal workflow related to this chapter and one point where an attacker could imitate a legitimate request. Then identify an independent verification method. This exercise turns awareness into an operational control. The objective is not to catch employees making mistakes; it is to discover where the business process makes a dangerous action too easy.

CHAPTER CHECK

Can you name the normal procedure, an independent verification channel and the incident-reporting route for this subject? If not, resolve that gap before an incident occurs.

5. Links, attachments and QR codes

Learning objective: understand the delivery mechanisms used to hide malicious destinations or content.

Why this matters

This chapter deals with the delivery mechanisms used to hide malicious destinations or content. Security incidents rarely depend on one spectacular technical trick. More often, an attacker combines ordinary information, a believable pretext and one action from a legitimate user. The employee's task is not to diagnose malware or perform forensics; it is to recognize when normal context has changed and to slow the transaction down long enough to verify it.

How the attack works

Attackers usually seek one of five outcomes: credentials, an authentication approval, execution of a file or action, disclosure of information, or redirection of a legitimate business process. The request can therefore look completely normal. Compare it with the expected workflow: who normally asks, through which channel, with which approvals, and at what stage of the process?

Warning signals

Useful signals include unexpected urgency, unusual secrecy, a new communication channel, a changed domain or payment detail, a request to bypass a control, a login you did not initiate, or pressure to act before verification. None of these proves an attack by itself. Their purpose is to trigger a verification step. Good awareness is disciplined uncertainty, not panic.

Realistic situations

Discuss these situations: a password-protected invoice archive; a QR re-authentication request; a document asking to disable protection. For each one, separate the business story from the evidence of identity. Ask whether the event was expected, whether it follows the normal process, whether the person can be confirmed using contact information already known to the organization, and what the consequence would be if you waited five minutes before acting.

Required behavior

The core practices are: confirm context before opening; never weaken security to view content; use approved sources. These controls must be connected to real company procedures. A policy that cannot be followed during ordinary work will eventually be bypassed, so managers must make the secure route clear and usable.

If you already made the mistake

Do not waste time trying to hide, undo or investigate the event alone. Record what happened, the approximate time, the device and service involved, and exactly what you entered, opened, approved, sent or changed. Contact the designated security channel immediately. Fast factual reporting may allow sessions to be revoked, transactions to be stopped, credentials to be reset or affected devices to be isolated.

Team exercise

Identify one normal workflow related to this chapter and one point where an attacker could imitate a legitimate request. Then identify an independent verification method. This exercise turns awareness into an operational control. The objective is not to catch employees making mistakes; it is to discover where the business process makes a dangerous action too easy.

CHAPTER CHECK

Can you name the normal procedure, an independent verification channel and the incident-reporting route for this subject? If not, resolve that gap before an incident occurs.

6. Social engineering

Learning objective: understand the exploitation of trust, authority, urgency, curiosity and helpfulness.

Why this matters

This chapter deals with the exploitation of trust, authority, urgency, curiosity and helpfulness. Security incidents rarely depend on one spectacular technical trick. More often, an attacker combines ordinary information, a believable pretext and one action from a legitimate user. The employee's task is not to diagnose malware or perform forensics; it is to recognize when normal context has changed and to slow the transaction down long enough to verify it.

How the attack works

Attackers usually seek one of five outcomes: credentials, an authentication approval, execution of a file or action, disclosure of information, or redirection of a legitimate business process. The request can therefore look completely normal. Compare it with the expected workflow: who normally asks, through which channel, with which approvals, and at what stage of the process?

Warning signals

Useful signals include unexpected urgency, unusual secrecy, a new communication channel, a changed domain or payment detail, a request to bypass a control, a login you did not initiate, or pressure to act before verification. None of these proves an attack by itself. Their purpose is to trigger a verification step. Good awareness is disciplined uncertainty, not panic.

Realistic situations

Discuss these situations: a fake technician; a caller who knows project names; a visitor tailgating through a secure door. For each one, separate the business story from the evidence of identity. Ask whether the event was expected, whether it follows the normal process, whether the person can be confirmed using contact information already known to the organization, and what the consequence would be if you waited five minutes before acting.

Required behavior

The core practices are: verify identity with official contact information; challenge unusual requests; reveal only necessary information. These controls must be connected to real company procedures. A policy that cannot be followed during ordinary work will eventually be bypassed, so managers must make the secure route clear and usable.

If you already made the mistake

Do not waste time trying to hide, undo or investigate the event alone. Record what happened, the approximate time, the device and service involved, and exactly what you entered, opened, approved, sent or changed. Contact the designated security channel immediately. Fast factual reporting may allow sessions to be revoked, transactions to be stopped, credentials to be reset or affected devices to be isolated.

Team exercise

Identify one normal workflow related to this chapter and one point where an attacker could imitate a legitimate request. Then identify an independent verification method. This exercise turns awareness into an operational control. The objective is not to catch employees making mistakes; it is to discover where the business process makes a dangerous action too easy.

CHAPTER CHECK

Can you name the normal procedure, an independent verification channel and the incident-reporting route for this subject? If not, resolve that gap before an incident occurs.

7. Business Email Compromise and payment fraud

Learning objective: understand the abuse of legitimate business processes to redirect money or sensitive data.

Why this matters

This chapter deals with the abuse of legitimate business processes to redirect money or sensitive data. Security incidents rarely depend on one spectacular technical trick. More often, an attacker combines ordinary information, a believable pretext and one action from a legitimate user. The employee's task is not to diagnose malware or perform forensics; it is to recognize when normal context has changed and to slow the transaction down long enough to verify it.

How the attack works

Attackers usually seek one of five outcomes: credentials, an authentication approval, execution of a file or action, disclosure of information, or redirection of a legitimate business process. The request can therefore look completely normal. Compare it with the expected workflow: who normally asks, through which channel, with which approvals, and at what stage of the process?

Warning signals

Useful signals include unexpected urgency, unusual secrecy, a new communication channel, a changed domain or payment detail, a request to bypass a control, a login you did not initiate, or pressure to act before verification. None of these proves an attack by itself. Their purpose is to trigger a verification step. Good awareness is disciplined uncertainty, not panic.

Realistic situations

Discuss these situations: a new supplier IBAN; a secret executive transfer; altered payment instructions inside a genuine thread. For each one, separate the business story from the evidence of identity. Ask whether the event was expected, whether it follows the normal process, whether the person can be confirmed using contact information already known to the organization, and what the consequence would be if you waited five minutes before acting.

Required behavior

The core practices are: use independent callbacks; require dual approval; preserve separation of duties. These controls must be connected to real company procedures. A policy that cannot be followed during ordinary work will eventually be bypassed, so managers must make the secure route clear and usable.

If you already made the mistake

Do not waste time trying to hide, undo or investigate the event alone. Record what happened, the approximate time, the device and service involved, and exactly what you entered, opened, approved, sent or changed. Contact the designated security channel immediately. Fast factual reporting may allow sessions to be revoked, transactions to be stopped, credentials to be reset or affected devices to be isolated.

Team exercise

Identify one normal workflow related to this chapter and one point where an attacker could imitate a legitimate request. Then identify an independent verification method. This exercise turns awareness into an operational control. The objective is not to catch employees making mistakes; it is to discover where the business process makes a dangerous action too easy.

CHAPTER CHECK

Can you name the normal procedure, an independent verification channel and the incident-reporting route for this subject? If not, resolve that gap before an incident occurs.

8. Workstation security

Learning objective: understand the protection of the trusted endpoint from which employees reach company systems.

Why this matters

This chapter deals with the protection of the trusted endpoint from which employees reach company systems. Security incidents rarely depend on one spectacular technical trick. More often, an attacker combines ordinary information, a believable pretext and one action from a legitimate user. The employee's task is not to diagnose malware or perform forensics; it is to recognize when normal context has changed and to slow the transaction down long enough to verify it.

How the attack works

Attackers usually seek one of five outcomes: credentials, an authentication approval, execution of a file or action, disclosure of information, or redirection of a legitimate business process. The request can therefore look completely normal. Compare it with the expected workflow: who normally asks, through which channel, with which approvals, and at what stage of the process?

Warning signals

Useful signals include unexpected urgency, unusual secrecy, a new communication channel, a changed domain or payment detail, a request to bypass a control, a login you did not initiate, or pressure to act before verification. None of these proves an attack by itself. Their purpose is to trigger a verification step. Good awareness is disciplined uncertainty, not panic.

Realistic situations

Discuss these situations: a free converter requesting admin rights; an over-privileged extension; a colleague borrowing an unlocked session. For each one, separate the business story from the evidence of identity. Ask whether the event was expected, whether it follows the normal process, whether the person can be confirmed using contact information already known to the organization, and what the consequence would be if you waited five minutes before acting.

Required behavior

The core practices are: lock the screen; patch promptly; use approved software. These controls must be connected to real company procedures. A policy that cannot be followed during ordinary work will eventually be bypassed, so managers must make the secure route clear and usable.

If you already made the mistake

Do not waste time trying to hide, undo or investigate the event alone. Record what happened, the approximate time, the device and service involved, and exactly what you entered, opened, approved, sent or changed. Contact the designated security channel immediately. Fast factual reporting may allow sessions to be revoked, transactions to be stopped, credentials to be reset or affected devices to be isolated.

Team exercise

Identify one normal workflow related to this chapter and one point where an attacker could imitate a legitimate request. Then identify an independent verification method. This exercise turns awareness into an operational control. The objective is not to catch employees making mistakes; it is to discover where the business process makes a dangerous action too easy.

CHAPTER CHECK

Can you name the normal procedure, an independent verification channel and the incident-reporting route for this subject? If not, resolve that gap before an incident occurs.

9. Mobile devices and messaging

Learning objective: understand the protection of portable devices that combine email, files, identity and MFA.

Why this matters

This chapter deals with the protection of portable devices that combine email, files, identity and MFA. Security incidents rarely depend on one spectacular technical trick. More often, an attacker combines ordinary information, a believable pretext and one action from a legitimate user. The employee's task is not to diagnose malware or perform forensics; it is to recognize when normal context has changed and to slow the transaction down long enough to verify it.

How the attack works

Attackers usually seek one of five outcomes: credentials, an authentication approval, execution of a file or action, disclosure of information, or redirection of a legitimate business process. The request can therefore look completely normal. Compare it with the expected workflow: who normally asks, through which channel, with which approvals, and at what stage of the process?

Warning signals

Useful signals include unexpected urgency, unusual secrecy, a new communication channel, a changed domain or payment detail, a request to bypass a control, a login you did not initiate, or pressure to act before verification. None of these proves an attack by itself. Their purpose is to trigger a verification step. Good awareness is disciplined uncertainty, not panic.

Realistic situations

Discuss these situations: parcel smishing; a colleague appearing from a new number; a lost work phone. For each one, separate the business story from the evidence of identity. Ask whether the event was expected, whether it follows the normal process, whether the person can be confirmed using contact information already known to the organization, and what the consequence would be if you waited five minutes before acting.

Required behavior

The core practices are: use a strong device lock; update promptly; use approved messaging. These controls must be connected to real company procedures. A policy that cannot be followed during ordinary work will eventually be bypassed, so managers must make the secure route clear and usable.

If you already made the mistake

Do not waste time trying to hide, undo or investigate the event alone. Record what happened, the approximate time, the device and service involved, and exactly what you entered, opened, approved, sent or changed. Contact the designated security channel immediately. Fast factual reporting may allow sessions to be revoked, transactions to be stopped, credentials to be reset or affected devices to be isolated.

Team exercise

Identify one normal workflow related to this chapter and one point where an attacker could imitate a legitimate request. Then identify an independent verification method. This exercise turns awareness into an operational control. The objective is not to catch employees making mistakes; it is to discover where the business process makes a dangerous action too easy.

CHAPTER CHECK

Can you name the normal procedure, an independent verification channel and the incident-reporting route for this subject? If not, resolve that gap before an incident occurs.

10. Remote work and travel

Learning objective: understand the additional risks created outside controlled company premises.

Why this matters

This chapter deals with the additional risks created outside controlled company premises. Security incidents rarely depend on one spectacular technical trick. More often, an attacker combines ordinary information, a believable pretext and one action from a legitimate user. The employee's task is not to diagnose malware or perform forensics; it is to recognize when normal context has changed and to slow the transaction down long enough to verify it.

How the attack works

Attackers usually seek one of five outcomes: credentials, an authentication approval, execution of a file or action, disclosure of information, or redirection of a legitimate business process. The request can therefore look completely normal. Compare it with the expected workflow: who normally asks, through which channel, with which approvals, and at what stage of the process?

Warning signals

Useful signals include unexpected urgency, unusual secrecy, a new communication channel, a changed domain or payment detail, a request to bypass a control, a login you did not initiate, or pressure to act before verification. None of these proves an attack by itself. Their purpose is to trigger a verification step. Good awareness is disciplined uncertainty, not panic.

Realistic situations

Discuss these situations: look-alike hotel Wi-Fi; an unattended conference laptop; a confidential screen visible on a train. For each one, separate the business story from the evidence of identity. Ask whether the event was expected, whether it follows the normal process, whether the person can be confirmed using contact information already known to the organization, and what the consequence would be if you waited five minutes before acting.

Required behavior

The core practices are: use approved remote access; retain physical control; protect screens and conversations. These controls must be connected to real company procedures. A policy that cannot be followed during ordinary work will eventually be bypassed, so managers must make the secure route clear and usable.

If you already made the mistake

Do not waste time trying to hide, undo or investigate the event alone. Record what happened, the approximate time, the device and service involved, and exactly what you entered, opened, approved, sent or changed. Contact the designated security channel immediately. Fast factual reporting may allow sessions to be revoked, transactions to be stopped, credentials to be reset or affected devices to be isolated.

Team exercise

Identify one normal workflow related to this chapter and one point where an attacker could imitate a legitimate request. Then identify an independent verification method. This exercise turns awareness into an operational control. The objective is not to catch employees making mistakes; it is to discover where the business process makes a dangerous action too easy.

CHAPTER CHECK

Can you name the normal procedure, an independent verification channel and the incident-reporting route for this subject? If not, resolve that gap before an incident occurs.

11. Data classification and safe sharing

Learning objective: understand the discipline of knowing what information you hold and who may receive it.

Why this matters

This chapter deals with the discipline of knowing what information you hold and who may receive it. Security incidents rarely depend on one spectacular technical trick. More often, an attacker combines ordinary information, a believable pretext and one action from a legitimate user. The employee's task is not to diagnose malware or perform forensics; it is to recognize when normal context has changed and to slow the transaction down long enough to verify it.

How the attack works

Attackers usually seek one of five outcomes: credentials, an authentication approval, execution of a file or action, disclosure of information, or redirection of a legitimate business process. The request can therefore look completely normal. Compare it with the expected workflow: who normally asks, through which channel, with which approvals, and at what stage of the process?

Warning signals

Useful signals include unexpected urgency, unusual secrecy, a new communication channel, a changed domain or payment detail, a request to bypass a control, a login you did not initiate, or pressure to act before verification. None of these proves an attack by itself. Their purpose is to trigger a verification step. Good awareness is disciplined uncertainty, not panic.

Realistic situations

Discuss these situations: hidden personal data in a spreadsheet; autocomplete selecting the wrong recipient; obsolete contractor access. For each one, separate the business story from the evidence of identity. Ask whether the event was expected, whether it follows the normal process, whether the person can be confirmed using contact information already known to the organization, and what the consequence would be if you waited five minutes before acting.

Required behavior

The core practices are: apply least privilege; check recipients and permissions; remove obsolete access. These controls must be connected to real company procedures. A policy that cannot be followed during ordinary work will eventually be bypassed, so managers must make the secure route clear and usable.

If you already made the mistake

Do not waste time trying to hide, undo or investigate the event alone. Record what happened, the approximate time, the device and service involved, and exactly what you entered, opened, approved, sent or changed. Contact the designated security channel immediately. Fast factual reporting may allow sessions to be revoked, transactions to be stopped, credentials to be reset or affected devices to be isolated.

Team exercise

Identify one normal workflow related to this chapter and one point where an attacker could imitate a legitimate request. Then identify an independent verification method. This exercise turns awareness into an operational control. The objective is not to catch employees making mistakes; it is to discover where the business process makes a dangerous action too easy.

CHAPTER CHECK

Can you name the normal procedure, an independent verification channel and the incident-reporting route for this subject? If not, resolve that gap before an incident occurs.

12. Cloud, SaaS and shadow IT

Learning objective: understand the governance of external services, storage, sharing and synchronization.

Why this matters

This chapter deals with the governance of external services, storage, sharing and synchronization. Security incidents rarely depend on one spectacular technical trick. More often, an attacker combines ordinary information, a believable pretext and one action from a legitimate user. The employee's task is not to diagnose malware or perform forensics; it is to recognize when normal context has changed and to slow the transaction down long enough to verify it.

How the attack works

Attackers usually seek one of five outcomes: credentials, an authentication approval, execution of a file or action, disclosure of information, or redirection of a legitimate business process. The request can therefore look completely normal. Compare it with the expected workflow: who normally asks, through which channel, with which approvals, and at what stage of the process?

Warning signals

Useful signals include unexpected urgency, unusual secrecy, a new communication channel, a changed domain or payment detail, a request to bypass a control, a login you did not initiate, or pressure to act before verification. None of these proves an attack by itself. Their purpose is to trigger a verification step. Good awareness is disciplined uncertainty, not panic.

Realistic situations

Discuss these situations: customer data on a free transfer site; a public link used for convenience; an old guest account. For each one, separate the business story from the evidence of identity. Ask whether the event was expected, whether it follows the normal process, whether the person can be confirmed using contact information already known to the organization, and what the consequence would be if you waited five minutes before acting.

Required behavior

The core practices are: use approved services; control guest access; avoid personal accounts. These controls must be connected to real company procedures. A policy that cannot be followed during ordinary work will eventually be bypassed, so managers must make the secure route clear and usable.

If you already made the mistake

Do not waste time trying to hide, undo or investigate the event alone. Record what happened, the approximate time, the device and service involved, and exactly what you entered, opened, approved, sent or changed. Contact the designated security channel immediately. Fast factual reporting may allow sessions to be revoked, transactions to be stopped, credentials to be reset or affected devices to be isolated.

Team exercise

Identify one normal workflow related to this chapter and one point where an attacker could imitate a legitimate request. Then identify an independent verification method. This exercise turns awareness into an operational control. The objective is not to catch employees making mistakes; it is to discover where the business process makes a dangerous action too easy.

CHAPTER CHECK

Can you name the normal procedure, an independent verification channel and the incident-reporting route for this subject? If not, resolve that gap before an incident occurs.

13. Generative AI

Learning objective: understand the confidentiality, privacy, intellectual-property and accuracy risks of AI assistants.

Why this matters

This chapter deals with the confidentiality, privacy, intellectual-property and accuracy risks of AI assistants. Security incidents rarely depend on one spectacular technical trick. More often, an attacker combines ordinary information, a believable pretext and one action from a legitimate user. The employee's task is not to diagnose malware or perform forensics; it is to recognize when normal context has changed and to slow the transaction down long enough to verify it.

How the attack works

Attackers usually seek one of five outcomes: credentials, an authentication approval, execution of a file or action, disclosure of information, or redirection of a legitimate business process. The request can therefore look completely normal. Compare it with the expected workflow: who normally asks, through which channel, with which approvals, and at what stage of the process?

Warning signals

Useful signals include unexpected urgency, unusual secrecy, a new communication channel, a changed domain or payment detail, a request to bypass a control, a login you did not initiate, or pressure to act before verification. None of these proves an attack by itself. Their purpose is to trigger a verification step. Good awareness is disciplined uncertainty, not panic.

Realistic situations

Discuss these situations: a contract uploaded for summarization; production secrets pasted with code; an invented policy citation. For each one, separate the business story from the evidence of identity. Ask whether the event was expected, whether it follows the normal process, whether the person can be confirmed using contact information already known to the organization, and what the consequence would be if you waited five minutes before acting.

Required behavior

The core practices are: use approved AI services; never submit credentials or restricted data; verify important outputs. These controls must be connected to real company procedures. A policy that cannot be followed during ordinary work will eventually be bypassed, so managers must make the secure route clear and usable.

If you already made the mistake

Do not waste time trying to hide, undo or investigate the event alone. Record what happened, the approximate time, the device and service involved, and exactly what you entered, opened, approved, sent or changed. Contact the designated security channel immediately. Fast factual reporting may allow sessions to be revoked, transactions to be stopped, credentials to be reset or affected devices to be isolated.

Team exercise

Identify one normal workflow related to this chapter and one point where an attacker could imitate a legitimate request. Then identify an independent verification method. This exercise turns awareness into an operational control. The objective is not to catch employees making mistakes; it is to discover where the business process makes a dangerous action too easy.

CHAPTER CHECK

Can you name the normal procedure, an independent verification channel and the incident-reporting route for this subject? If not, resolve that gap before an incident occurs.

14. Social media and public information

Learning objective: understand the reconnaissance value of apparently harmless public details.

Why this matters

This chapter deals with the reconnaissance value of apparently harmless public details. Security incidents rarely depend on one spectacular technical trick. More often, an attacker combines ordinary information, a believable pretext and one action from a legitimate user. The employee's task is not to diagnose malware or perform forensics; it is to recognize when normal context has changed and to slow the transaction down long enough to verify it.

How the attack works

Attackers usually seek one of five outcomes: credentials, an authentication approval, execution of a file or action, disclosure of information, or redirection of a legitimate business process. The request can therefore look completely normal. Compare it with the expected workflow: who normally asks, through which channel, with which approvals, and at what stage of the process?

Warning signals

Useful signals include unexpected urgency, unusual secrecy, a new communication channel, a changed domain or payment detail, a request to bypass a control, a login you did not initiate, or pressure to act before verification. None of these proves an attack by itself. Their purpose is to trigger a verification step. Good awareness is disciplined uncertainty, not panic.

Realistic situations

Discuss these situations: a badge visible in a conference photo; executive travel announced publicly; probing questions from a recruiter. For each one, separate the business story from the evidence of identity. Ask whether the event was expected, whether it follows the normal process, whether the person can be confirmed using contact information already known to the organization, and what the consequence would be if you waited five minutes before acting.

Required behavior

The core practices are: review posts and images; limit technical detail; use approved corporate communications. These controls must be connected to real company procedures. A policy that cannot be followed during ordinary work will eventually be bypassed, so managers must make the secure route clear and usable.

If you already made the mistake

Do not waste time trying to hide, undo or investigate the event alone. Record what happened, the approximate time, the device and service involved, and exactly what you entered, opened, approved, sent or changed. Contact the designated security channel immediately. Fast factual reporting may allow sessions to be revoked, transactions to be stopped, credentials to be reset or affected devices to be isolated.

Team exercise

Identify one normal workflow related to this chapter and one point where an attacker could imitate a legitimate request. Then identify an independent verification method. This exercise turns awareness into an operational control. The objective is not to catch employees making mistakes; it is to discover where the business process makes a dangerous action too easy.

CHAPTER CHECK

Can you name the normal procedure, an independent verification channel and the incident-reporting route for this subject? If not, resolve that gap before an incident occurs.

15. Physical security

Learning objective: understand the protection of offices, devices, badges, documents and removable media.

Why this matters

This chapter deals with the protection of offices, devices, badges, documents and removable media. Security incidents rarely depend on one spectacular technical trick. More often, an attacker combines ordinary information, a believable pretext and one action from a legitimate user. The employee's task is not to diagnose malware or perform forensics; it is to recognize when normal context has changed and to slow the transaction down long enough to verify it.

How the attack works

Attackers usually seek one of five outcomes: credentials, an authentication approval, execution of a file or action, disclosure of information, or redirection of a legitimate business process. The request can therefore look completely normal. Compare it with the expected workflow: who normally asks, through which channel, with which approvals, and at what stage of the process?

Warning signals

Useful signals include unexpected urgency, unusual secrecy, a new communication channel, a changed domain or payment detail, a request to bypass a control, a login you did not initiate, or pressure to act before verification. None of these proves an attack by itself. Their purpose is to trigger a verification step. Good awareness is disciplined uncertainty, not panic.

Realistic situations

Discuss these situations: tailgating; payroll pages left on a printer; a USB drive found in a parking area. For each one, separate the business story from the evidence of identity. Ask whether the event was expected, whether it follows the normal process, whether the person can be confirmed using contact information already known to the organization, and what the consequence would be if you waited five minutes before acting.

Required behavior

The core practices are: protect badges; escort visitors; secure printing and disposal. These controls must be connected to real company procedures. A policy that cannot be followed during ordinary work will eventually be bypassed, so managers must make the secure route clear and usable.

If you already made the mistake

Do not waste time trying to hide, undo or investigate the event alone. Record what happened, the approximate time, the device and service involved, and exactly what you entered, opened, approved, sent or changed. Contact the designated security channel immediately. Fast factual reporting may allow sessions to be revoked, transactions to be stopped, credentials to be reset or affected devices to be isolated.

Team exercise

Identify one normal workflow related to this chapter and one point where an attacker could imitate a legitimate request. Then identify an independent verification method. This exercise turns awareness into an operational control. The objective is not to catch employees making mistakes; it is to discover where the business process makes a dangerous action too easy.

CHAPTER CHECK

Can you name the normal procedure, an independent verification channel and the incident-reporting route for this subject? If not, resolve that gap before an incident occurs.

16. Updates and software hygiene

Learning objective: understand the reduction of known vulnerabilities through controlled software and timely patching.

Why this matters

This chapter deals with the reduction of known vulnerabilities through controlled software and timely patching. Security incidents rarely depend on one spectacular technical trick. More often, an attacker combines ordinary information, a believable pretext and one action from a legitimate user. The employee's task is not to diagnose malware or perform forensics; it is to recognize when normal context has changed and to slow the transaction down long enough to verify it.

How the attack works

Attackers usually seek one of five outcomes: credentials, an authentication approval, execution of a file or action, disclosure of information, or redirection of a legitimate business process. The request can therefore look completely normal. Compare it with the expected workflow: who normally asks, through which channel, with which approvals, and at what stage of the process?

Warning signals

Useful signals include unexpected urgency, unusual secrecy, a new communication channel, a changed domain or payment detail, a request to bypass a control, a login you did not initiate, or pressure to act before verification. None of these proves an attack by itself. Their purpose is to trigger a verification step. Good awareness is disciplined uncertainty, not panic.

Realistic situations

Discuss these situations: a fake codec download; an old app requiring disabled security; months of postponed updates. For each one, separate the business story from the evidence of identity. Ask whether the event was expected, whether it follows the normal process, whether the person can be confirmed using contact information already known to the organization, and what the consequence would be if you waited five minutes before acting.

Required behavior

The core practices are: use approved software; patch and restart on time; escalate compatibility problems. These controls must be connected to real company procedures. A policy that cannot be followed during ordinary work will eventually be bypassed, so managers must make the secure route clear and usable.

If you already made the mistake

Do not waste time trying to hide, undo or investigate the event alone. Record what happened, the approximate time, the device and service involved, and exactly what you entered, opened, approved, sent or changed. Contact the designated security channel immediately. Fast factual reporting may allow sessions to be revoked, transactions to be stopped, credentials to be reset or affected devices to be isolated.

Team exercise

Identify one normal workflow related to this chapter and one point where an attacker could imitate a legitimate request. Then identify an independent verification method. This exercise turns awareness into an operational control. The objective is not to catch employees making mistakes; it is to discover where the business process makes a dangerous action too easy.

CHAPTER CHECK

Can you name the normal procedure, an independent verification channel and the incident-reporting route for this subject? If not, resolve that gap before an incident occurs.

17. Incident recognition and reporting

Learning objective: understand the rapid escalation of suspicious events, mistakes, losses and unexpected access.

Why this matters

This chapter deals with the rapid escalation of suspicious events, mistakes, losses and unexpected access. Security incidents rarely depend on one spectacular technical trick. More often, an attacker combines ordinary information, a believable pretext and one action from a legitimate user. The employee's task is not to diagnose malware or perform forensics; it is to recognize when normal context has changed and to slow the transaction down long enough to verify it.

How the attack works

Attackers usually seek one of five outcomes: credentials, an authentication approval, execution of a file or action, disclosure of information, or redirection of a legitimate business process. The request can therefore look completely normal. Compare it with the expected workflow: who normally asks, through which channel, with which approvals, and at what stage of the process?

Warning signals

Useful signals include unexpected urgency, unusual secrecy, a new communication channel, a changed domain or payment detail, a request to bypass a control, a login you did not initiate, or pressure to act before verification. None of these proves an attack by itself. Their purpose is to trigger a verification step. Good awareness is disciplined uncertainty, not panic.

Realistic situations

Discuss these situations: credentials entered on the wrong domain; a sensitive attachment sent to the wrong person; accidental MFA approval. For each one, separate the business story from the evidence of identity. Ask whether the event was expected, whether it follows the normal process, whether the person can be confirmed using contact information already known to the organization, and what the consequence would be if you waited five minutes before acting.

Required behavior

The core practices are: report facts and time; preserve evidence; follow response instructions. These controls must be connected to real company procedures. A policy that cannot be followed during ordinary work will eventually be bypassed, so managers must make the secure route clear and usable.

If you already made the mistake

Do not waste time trying to hide, undo or investigate the event alone. Record what happened, the approximate time, the device and service involved, and exactly what you entered, opened, approved, sent or changed. Contact the designated security channel immediately. Fast factual reporting may allow sessions to be revoked, transactions to be stopped, credentials to be reset or affected devices to be isolated.

Team exercise

Identify one normal workflow related to this chapter and one point where an attacker could imitate a legitimate request. Then identify an independent verification method. This exercise turns awareness into an operational control. The objective is not to catch employees making mistakes; it is to discover where the business process makes a dangerous action too easy.

CHAPTER CHECK

Can you name the normal procedure, an independent verification channel and the incident-reporting route for this subject? If not, resolve that gap before an incident occurs.

18. Building a durable security culture

Learning objective: understand the everyday behavior that remains when nobody is watching.

Why this matters

This chapter deals with the everyday behavior that remains when nobody is watching. Security incidents rarely depend on one spectacular technical trick. More often, an attacker combines ordinary information, a believable pretext and one action from a legitimate user. The employee's task is not to diagnose malware or perform forensics; it is to recognize when normal context has changed and to slow the transaction down long enough to verify it.

How the attack works

Attackers usually seek one of five outcomes: credentials, an authentication approval, execution of a file or action, disclosure of information, or redirection of a legitimate business process. The request can therefore look completely normal. Compare it with the expected workflow: who normally asks, through which channel, with which approvals, and at what stage of the process?

Warning signals

Useful signals include unexpected urgency, unusual secrecy, a new communication channel, a changed domain or payment detail, a request to bypass a control, a login you did not initiate, or pressure to act before verification. None of these proves an attack by itself. Their purpose is to trigger a verification step. Good awareness is disciplined uncertainty, not panic.

Realistic situations

Discuss these situations: a junior employee verifying an executive request; a team reporting a near miss; a simulation exposing a bad workflow. For each one, separate the business story from the evidence of identity. Ask whether the event was expected, whether it follows the normal process, whether the person can be confirmed using contact information already known to the organization, and what the consequence would be if you waited five minutes before acting.

Required behavior

The core practices are: reward early reporting; remove risky workarounds; train repeatedly. These controls must be connected to real company procedures. A policy that cannot be followed during ordinary work will eventually be bypassed, so managers must make the secure route clear and usable.

If you already made the mistake

Do not waste time trying to hide, undo or investigate the event alone. Record what happened, the approximate time, the device and service involved, and exactly what you entered, opened, approved, sent or changed. Contact the designated security channel immediately. Fast factual reporting may allow sessions to be revoked, transactions to be stopped, credentials to be reset or affected devices to be isolated.

Team exercise

Identify one normal workflow related to this chapter and one point where an attacker could imitate a legitimate request. Then identify an independent verification method. This exercise turns awareness into an operational control. The objective is not to catch employees making mistakes; it is to discover where the business process makes a dangerous action too easy.

CHAPTER CHECK

Can you name the normal procedure, an independent verification channel and the incident-reporting route for this subject? If not, resolve that gap before an incident occurs.

The first 15 minutes after a security mistake

Stop further interaction. Do not delete evidence unless instructed. Note the time and exactly what you did. Contact the designated security channel immediately. If credentials were entered, say so explicitly. If money or bank details were involved, use the financial-fraud escalation route at once. If a device is lost, report the device and the accounts accessible from it. Follow the response team's instructions rather than improvising. Speed matters because sessions, credentials and transactions may still be reversible.

Practical discussion

Managers should review this page with their teams and replace generic references such as 'designated security channel' with the organization's real contact method, escalation route and expected response time. Employees should leave the session knowing exactly what to do, not merely what to fear.

TAKEAWAY

Security works when the safe action is clear, practical and supported by the organization.

Daily employee security checklist

At login: am I using the expected service and did I initiate this MFA request? In email: do sender, domain, context and requested action make sense? Before sending: have I checked recipients, attachments, classification and permissions? Before installing: is the software approved? When leaving: is the session locked? When travelling: is the device under my control? With AI or cloud tools: is this service authorized for this information? When uncertain: do I know exactly where to report?

Practical discussion

Managers should review this page with their teams and replace generic references such as 'designated security channel' with the organization's real contact method, escalation route and expected response time. Employees should leave the session knowing exactly what to do, not merely what to fear.

TAKEAWAY

Security works when the safe action is clear, practical and supported by the organization.

Twenty mistakes to avoid

Reusing passwords; sharing credentials; approving unexpected MFA; reading a one-time code to a caller; clicking because a message is urgent; trusting a display name; accepting a bank-detail change by email alone; enabling macros because a document requests it; scanning an unknown QR code; installing unapproved software; disabling endpoint protection; using personal cloud storage for company files; creating public links unnecessarily; leaving a session unlocked; plugging in found USB media; exposing confidential screens in public; oversharing internal information online; sending restricted data to an unapproved AI service; delaying incident reporting; hiding a mistake.

Practical discussion

Managers should review this page with their teams and replace generic references such as 'designated security channel' with the organization's real contact method, escalation route and expected response time. Employees should leave the session knowing exactly what to do, not merely what to fear.

TAKEAWAY

Security works when the safe action is clear, practical and supported by the organization.

Employee Security Charter

I protect my credentials and authentication methods. I use approved systems and respect access rights. I verify sensitive or unusual requests through an independent trusted channel. I protect confidential and personal information throughout its lifecycle. I do not deliberately bypass security controls for convenience. I keep company devices physically secure. I use cloud and AI services according to policy. I promptly report suspicious activity, accidental disclosure, device loss and mistakes. I support colleagues who choose to verify rather than rush. Cybersecurity is a shared professional responsibility.

Practical discussion

Managers should review this page with their teams and replace generic references such as 'designated security channel' with the organization's real contact method, escalation route and expected response time. Employees should leave the session knowing exactly what to do, not merely what to fear.

TAKEAWAY

Security works when the safe action is clear, practical and supported by the organization.

Final knowledge check

An executive asks you to bypass a payment control: follow the normal approval process. You receive MFA you did not initiate: reject and report. A real supplier thread contains new bank details: verify independently. You entered a password on a suspicious page: report immediately. A free AI tool can summarize a customer contract: only use it if the service and that data use are explicitly authorized. A colleague challenges an unusual senior request: that verification is part of the control system.

Practical discussion

Managers should review this page with their teams and replace generic references such as 'designated security channel' with the organization's real contact method, escalation route and expected response time. Employees should leave the session knowing exactly what to do, not merely what to fear.

TAKEAWAY

Security works when the safe action is clear, practical and supported by the organization.

Reference framework

This handbook is aligned conceptually with public awareness and security guidance from CNIL, ENISA, NIST and CISA. CNIL emphasizes involving and training users, authentication, workstation and mobile security, cloud and AI considerations. NIST's Phish Scale work emphasizes the human difficulty of detecting phishing and the importance of context in awareness programs. CISA awareness material emphasizes phishing recognition and reporting, strong passwords, MFA and software updates. Each organization must adapt the handbook to its own law, contracts, systems, contacts and incident procedures.

Practical discussion

Managers should review this page with their teams and replace generic references such as 'designated security channel' with the organization's real contact method, escalation route and expected response time. Employees should leave the session knowing exactly what to do, not merely what to fear.

TAKEAWAY

Security works when the safe action is clear, practical and supported by the organization.