# CYBER SECURITY STARTER KIT

Protect yourself online in 7 days.
Proteggiti online in 7 giorni.

**BILINGUAL PRACTICAL EDITION · EN + IT · 7 DAYS**

An expanded educational workbook built from the seven-chapter Starter Kit supplied for CyberNext Academy.
Free educational resource. Practical guidance for everyday digital safety; not legal, forensic or incident-response advice.

# Seven days. Seven improvements.

The best security routine is the one you will actually maintain. This short workbook focuses on the most useful habits for everyday accounts and devices: unique passwords, multifactor authentication, skepticism about unexpected messages, updates and reliable backups.

Each day includes a simple explanation, concrete actions and a worksheet. You do not need to be a technical expert. Choose one manageable improvement and move to the next only after checking that it works.

The activities are defensive and suitable for your own devices and accounts. Never investigate accounts or systems that do not belong to you without explicit permission.

## How to use this kit

Read the English or Italian version of the daily lesson. Then use the combined action worksheet to perform the tasks and record what changed. Revisit the last-day checklist at least once a month.

This is a practical starting point, not a guarantee of protection. Security recommendations can change as technology evolves; review the settings and guidance of each service you use.

# Sette giorni. Sette miglioramenti.

La routine di sicurezza migliore è quella che riuscirai davvero a mantenere. Questa guida si concentra sulle abitudini più utili per account e dispositivi: password uniche, autenticazione a più fattori, verifica dei messaggi inattesi, aggiornamenti e backup affidabili.

Ogni giorno trovi una spiegazione essenziale, azioni concrete e una scheda di lavoro. Non servono competenze tecniche avanzate: scegli un miglioramento alla volta e controlla che funzioni prima di proseguire.

Le attività sono difensive e riguardano i tuoi account e dispositivi. Non indagare su sistemi o account altrui senza un’autorizzazione esplicita.

## Come usare questa guida

Leggi la versione italiana o inglese della lezione quotidiana. Utilizza poi la scheda operativa bilingue per svolgere le attività e registrare le modifiche. Ripeti la checklist dell’ultimo giorno almeno una volta al mese.

È un punto di partenza pratico, non una garanzia assoluta. Le raccomandazioni cambiano con la tecnologia: consulta periodicamente le impostazioni e le indicazioni dei servizi che utilizzi.

YOUR LEARNING MAP / INDICE

# One focused step per day.


DAY 01 / GIORNO 01

Common threats · Le minacce più comuni

DAY 02 / GIORNO 02

Passwords and MFA · Password e autenticazione a più fattori

DAY 03 / GIORNO 03

Phishing anatomy · Come riconoscere il phishing

DAY 04 / GIORNO 04

Safer browsing · Navigazione più sicura

DAY 05 / GIORNO 05

Smartphone security · Sicurezza dello smartphone

DAY 06 / GIORNO 06

Backups that restore · Backup che funzionano davvero

DAY 07 / GIORNO 07

Your 30-minute checklist · Checklist di sicurezza in 30 minuti


## Daily rhythm / Routine quotidiana

01 Read / Leggi · 02 Act / Agisci · 03 Verify / Verifica · 04 Record / Annota

# Common threats

Recognize the five patterns that most often lead to avoidable account incidents.

## Phishing and social engineering

A suspicious message can imitate a colleague, delivery service or bank. The goal is often to make you act before verifying. Look for unexpected requests for passwords, verification codes, payments or attachments. Do not rely on the sender display name alone.

## Credential theft and account takeover

An attacker may reuse credentials exposed in an unrelated breach. A unique password for each important account, combined with multi-factor authentication, reduces the chance that a single incident spreads to other services.

## Malware and risky downloads

Applications from unknown sources, unexpected attachments and outdated software can place devices at risk. Install updates, review permissions and avoid running unfamiliar files. Security software is helpful, but it does not replace careful decisions.

## Today’s outcome / Learning objective

After this lesson you should be able to explain the main risk in your own words and name one practical improvement you can make today.

# Le minacce più comuni

Riconosci cinque schemi ricorrenti che possono compromettere gli account.

## Phishing e ingegneria sociale

Un messaggio sospetto può imitare una collega, un corriere o una banca. Lo scopo è spingerti ad agire prima della verifica. Diffida delle richieste inattese di password, codici, pagamenti o allegati. Il nome visualizzato del mittente non basta per stabilire l’autenticità.

## Furto di credenziali e accessi non autorizzati

Le password diffuse in una violazione possono essere provate su altri servizi. Credenziali diverse per ogni account importante e autenticazione a più fattori riducono il rischio che un problema coinvolga tutti i tuoi accessi.

## Malware e download rischiosi

Applicazioni da fonti incerte, allegati inattesi e software non aggiornati possono mettere a rischio i dispositivi. Installa gli aggiornamenti, controlla i permessi e non aprire file sconosciuti. Gli strumenti di sicurezza non sostituiscono l’attenzione.

## Obiettivo di oggi

Dopo questa lezione, prova a spiegare il rischio con parole tue e scegli un intervento pratico da completare.

DAY 01 / GIORNO 01 · WORKSHEET

# Your security action plan

## Action list / Lista delle azioni

☐ TASK 01

Identify three unexpected messages you received recently; check what each asked you to do.

Individua tre messaggi inattesi ricevuti di recente e valuta cosa ti chiedevano.

☐ TASK 02

Verify one official contact channel for an important service.

Salva un canale ufficiale di contatto per un servizio importante.

☐ TASK 03

Review sign-in alerts for your primary email account.

Controlla gli avvisi di accesso della tua casella email principale.

## What did you change? / Che cosa hai modificato?

_____

_____

_____

Next review date / Prossimo controllo: _____

DAY 02 / ENGLISH LESSON

# Passwords and MFA

Build an account system you can maintain without reusing passwords.

## Unique credentials

Use a long, unique password for every important service. A password manager can generate and store credentials so you do not need to memorize dozens of variations. Prioritize email, banking, cloud storage and the manager itself.

## MFA and passkeys

Enable multi-factor authentication wherever available. Authenticator apps, security keys and passkeys can offer stronger protection against phishing than SMS in many situations. Choose methods supported by your accounts and understand how to recover access.

## Recovery matters

Store backup codes in a secure place separate from your main device. Review recovery emails and phone numbers, and remove old devices from account settings. Try a safe recovery rehearsal so you do not discover a missing code during an emergency.

## Today’s outcome / Learning objective

After this lesson you should be able to explain the main risk in your own words and name one practical improvement you can make today.

# Password e autenticazione a più fattori

Crea un sistema gestibile senza riutilizzare le password.

## Credenziali uniche

Usa password lunghe e diverse per ogni servizio importante. Un gestore di password può creare e conservare le credenziali, evitando decine di varianti difficili da ricordare. Dai priorità a email, servizi finanziari, cloud e al gestore stesso.

## MFA e passkey

Attiva l’autenticazione a più fattori dove possibile. App di autenticazione, chiavi di sicurezza e passkey possono offrire una maggiore resistenza al phishing rispetto agli SMS, in diversi contesti. Scegli i metodi supportati e pianifica il recupero.

## Il recupero è essenziale

Conserva i codici di emergenza in un luogo sicuro e separato dal dispositivo principale. Controlla email e numeri di recupero e rimuovi i dispositivi vecchi dagli account. Verifica la procedura prima di averne urgentemente bisogno.

## Obiettivo di oggi

Dopo questa lezione, prova a spiegare il rischio con parole tue e scegli un intervento pratico da completare.

# Your security action plan

## Action list / Lista delle azioni

☐ TASK 01

Install or review a reputable password manager.

Installa o controlla un gestore di password affidabile.

☐ TASK 02

Change one reused password on a critical account.

Sostituisci una password riutilizzata su un account critico.

☐ TASK 03

Enable MFA and securely store recovery codes.

Attiva MFA e conserva i codici di recupero in sicurezza.

## What did you change? / Che cosa hai modificato?

_____

_____

_____

Next review date / Prossimo controllo: _____

DAY 03 / ENGLISH LESSON

# Phishing anatomy

Learn a repeatable way to decide whether to trust an unexpected message.

## Pressure and impersonation

Scammers create artificial urgency: “Your account will close today” or “Payment failed.” They may spoof company names or use a copied logo. Slow down and focus on the action being requested instead of the visual appearance.

## Links and attachments

A button can hide a destination different from its label. On a trusted device, inspect the visible domain, but do not assume a plausible-looking domain is safe. Avoid opening unexpected attachments or enabling document macros.

## Independent verification

Open the official app or type the address from a known source. If a colleague asks for money or credentials, contact them using a separate trusted channel. Never share one-time login codes with someone who approaches you.

## Today’s outcome / Learning objective

After this lesson you should be able to explain the main risk in your own words and name one practical improvement you can make today.

# Come riconoscere il phishing

Impara a verificare una richiesta inattesa prima di agire.

## Pressione e imitazione

I truffatori creano urgenza artificiale: «Il tuo account sarà chiuso oggi» o «Pagamento non riuscito». Possono imitare nomi e loghi aziendali. Rallenta e valuta l’azione richiesta, non soltanto l’aspetto del messaggio.

## Link e allegati

Un pulsante può nascondere una destinazione diversa dal testo visualizzato. Controlla il dominio quando è possibile farlo in sicurezza, senza supporre che un nome plausibile sia necessariamente autentico. Evita allegati inattesi e macro sconosciute.

## Verifica indipendente

Apri l’app ufficiale oppure digita un indirizzo conosciuto. Se una persona ti chiede denaro o credenziali, contattala tramite un secondo canale affidabile. Non condividere mai codici di accesso temporanei con chi ti cerca spontaneamente.

## Obiettivo di oggi

Dopo questa lezione, prova a spiegare il rischio con parole tue e scegli un intervento pratico da completare.

DAY 03 / GIORNO 03 · WORKSHEET

# Your security action plan

## Action list / Lista delle azioni

☐ TASK 01

Choose a suspicious message and list two red flags without clicking it.

Scegli un messaggio sospetto e individua due segnali di rischio senza aprirne i link.

☐ TASK 02

Open the relevant service independently and check if the request is real.

Accedi al servizio in modo indipendente e verifica la richiesta.

☐ TASK 03

Report the suspicious message using the service’s official reporting option.

Segnala il messaggio attraverso il canale ufficiale.

## What did you change? / Che cosa hai modificato?

_____

_____

_____

Next review date / Prossimo controllo: _____

DAY 04 / ENGLISH LESSON

# Safer browsing

Use browser updates, careful permissions and realistic expectations about VPNs.

## Patch first

Keep your operating system, browser and apps up to date. Many successful attacks rely on known flaws after fixes are already available. Automatic updates are useful when the device remains supported.

## Extensions and permissions

Browser extensions can read pages or change browsing behavior. Remove unused add-ons and review permissions for any extension you keep. Limit unnecessary access to location, microphone and camera.

## HTTPS, DNS and VPNs

HTTPS protects the connection, not the trustworthiness of a merchant or message. DNS protections can help block some known malicious domains. A VPN changes the route of your traffic but does not stop phishing, unsafe downloads or account takeover.

## Today’s outcome / Learning objective

After this lesson you should be able to explain the main risk in your own words and name one practical improvement you can make today.

GIORNO 04 / LEZIONE IN ITALIANO

# Navigazione più sicura

Aggiornamenti, permessi e aspettative realistiche sulle VPN.

## Prima gli aggiornamenti

Mantieni aggiornati sistema operativo, browser e applicazioni. Molti incidenti sfruttano vulnerabilità note per le quali esistono già correzioni. Gli aggiornamenti automatici aiutano quando il dispositivo è ancora supportato.

## Estensioni e permessi

Le estensioni possono leggere pagine o modificare la navigazione. Elimina i componenti inutilizzati e controlla i permessi di quelli che conservi. Limita gli accessi non necessari a posizione, microfono e fotocamera.

## HTTPS, DNS e VPN

HTTPS protegge la connessione, ma non garantisce l’affidabilità del sito. Alcuni sistemi DNS aiutano a bloccare domini malevoli conosciuti. Una VPN modifica il percorso del traffico ma non impedisce phishing, download pericolosi o furti di account.

## Obiettivo di oggi

Dopo questa lezione, prova a spiegare il rischio con parole tue e scegli un intervento pratico da completare.

# Your security action plan

## Action list / Lista delle azioni

☐ TASK 01

Install pending browser and operating-system updates.

Installa gli aggiornamenti in sospeso di browser e sistema operativo.

☐ TASK 02

Remove one unused browser extension and review remaining permissions.

Rimuovi un’estensione inutilizzata e verifica i permessi delle altre.

☐ TASK 03

Check whether you are assuming too much protection from a VPN.

Controlla se attribuisci alla VPN protezioni che non offre.

## What did you change? / Che cosa hai modificato?

_____

_____

_____

Next review date / Prossimo controllo: _____

DAY 05 / ENGLISH LESSON

# Smartphone security

Make the device harder to misuse after loss, theft or accidental sharing.

## Device lock and updates

Use a strong device unlock method and automatic security updates. A short PIN is convenient but easier to observe or guess. Enable device encryption where supported; many modern phones encrypt data by default.

## App hygiene

Install applications from reputable sources and avoid giving broad permissions without a reason. Remove apps you no longer use. Review location, contacts, photos, microphone and camera access periodically.

## Account and loss recovery

Review the account linked to your phone and secure it with MFA. Configure trusted device-location and remote-lock features if available. Ensure important photos and files are backed up before a device is lost.

## Today’s outcome / Learning objective

After this lesson you should be able to explain the main risk in your own words and name one practical improvement you can make today.

GIORNO 05 / LEZIONE IN ITALIANO

# Sicurezza dello smartphone

Riduci i rischi in caso di smarrimento, furto o condivisione accidentale.

## Blocco e aggiornamenti

Usa un metodo di sblocco robusto e aggiornamenti di sicurezza automatici. Un PIN molto breve è comodo ma più facile da osservare o indovinare. Attiva la cifratura quando disponibile; molti telefoni moderni la usano già.

## Igiene delle app

Installa applicazioni da fonti affidabili e non concedere permessi ampi senza necessità. Elimina quelle che non usi. Controlla periodicamente accessi a posizione, contatti, foto, microfono e fotocamera.

## Recupero in caso di perdita

Proteggi con MFA l’account collegato al telefono. Configura funzioni affidabili di localizzazione e blocco remoto, se presenti. Assicurati che foto e file importanti abbiano un backup prima dello smarrimento.

## Obiettivo di oggi

Dopo questa lezione, prova a spiegare il rischio con parole tue e scegli un intervento pratico da completare.

DAY 05 / GIORNO 05 · WORKSHEET

# Your security action plan

## Action list / Lista delle azioni

☐ TASK 01

Change an overly simple device PIN, if needed.

Se necessario, sostituisci un PIN troppo semplice.

☐ TASK 02

Review permissions of three installed apps.

Controlla i permessi di tre app installate.

☐ TASK 03

Check backup status and how to remotely lock a lost device.

Verifica il backup e le istruzioni per bloccare da remoto un telefono perso.

## What did you change? / Che cosa hai modificato?

_____

_____

_____

Next review date / Prossimo controllo: _____

DAY 06 / ENGLISH LESSON

# Backups that restore

Protect irreplaceable files with independent copies and recovery testing.

## The 3-2-1 principle

A common strategy is three copies of important data, using two different storage types, with one copy kept off-site or offline. The exact arrangement depends on your devices, privacy needs and budget.

## Separation protects recovery

If every backup stays connected to the same device or account, accidental deletion and malware may affect them all. A disconnected drive or separately protected cloud account can reduce that risk.

## Practice restoration

A backup that cannot be restored is not dependable. Try recovering a sample file to a safe folder. Document the location of your backups, recovery credentials and when each copy was last checked.

## Today’s outcome / Learning objective

After this lesson you should be able to explain the main risk in your own words and name one practical improvement you can make today.

# Backup che funzionano davvero

Proteggi i file importanti con copie separate e prove di ripristino.

## Il principio 3-2-1

Una strategia comune prevede tre copie dei dati importanti, su due tipologie di supporto, con una copia conservata altrove oppure offline. La soluzione concreta dipende dai dispositivi, dalla privacy e dal budget.

## Separare per recuperare

Se ogni copia resta collegata allo stesso dispositivo o account, cancellazioni accidentali e malware possono colpirle tutte. Un disco scollegato o un account cloud protetto separatamente possono ridurre il rischio.

## Prova il ripristino

Un backup impossibile da ripristinare non è affidabile. Recupera un file campione in una cartella sicura. Registra dove si trovano le copie, come accedervi e quando le hai controllate l’ultima volta.

## Obiettivo di oggi

Dopo questa lezione, prova a spiegare il rischio con parole tue e scegli un intervento pratico da completare.

DAY 06 / GIORNO 06 · WORKSHEET

# Your security action plan

## Action list / Lista delle azioni

☐ TASK 01

List the folders or documents you cannot afford to lose.

Elenca le cartelle e i documenti che non puoi permetterti di perdere.

☐ TASK 02

Check whether a backup copy is independent from your main device.

Controlla che almeno una copia sia indipendente dal dispositivo principale.

☐ TASK 03

Restore one harmless file and record the result.

Ripristina un file di prova e annota il risultato.

## What did you change? / Che cosa hai modificato?

_____

_____

_____

Next review date / Prossimo controllo: _____

DAY 07 / ENGLISH LESSON

# Your 30-minute checklist

Turn the previous chapters into a practical maintenance routine.

## First ten minutes: accounts

Check that your main email uses a unique password and MFA. Review recovery contacts and remove unfamiliar active sessions. If you find a session you do not recognize, follow the service’s official incident guidance.

## Next ten minutes: devices

Check updates, screen locks, installed extensions and unnecessary permissions. Focus on the devices and accounts you use for work, finances and communication.

## Final ten minutes: continuity

Confirm that important files have an independent backup. Save recovery information securely and write down where you will look for help if an account or device becomes inaccessible.

## Today’s outcome / Learning objective

After this lesson you should be able to explain the main risk in your own words and name one practical improvement you can make today.

# Checklist di sicurezza in 30 minuti

Trasforma i capitoli precedenti in una routine semplice.

## Primi dieci minuti: account

Verifica che la tua email principale abbia una password unica e MFA. Controlla i contatti di recupero e le sessioni attive sconosciute. Se trovi un accesso anomalo, segui le istruzioni ufficiali del servizio.

## Dieci minuti successivi: dispositivi

Controlla aggiornamenti, blocco schermo, estensioni installate e permessi non necessari. Concentrati sui dispositivi e sugli account che usi per lavoro, finanze e comunicazioni.

## Ultimi dieci minuti: continuità

Assicurati che i file importanti abbiano un backup indipendente. Conserva in sicurezza le informazioni per il recupero e annota dove cercare assistenza se perdi l’accesso a un account o dispositivo.

## Obiettivo di oggi

Dopo questa lezione, prova a spiegare il rischio con parole tue e scegli un intervento pratico da completare.

DAY 07 / GIORNO 07 · WORKSHEET

# Your security action plan

## Action list / Lista delle azioni

☐ TASK 01

Enable or check MFA for your main email and a financial account.

Controlla MFA sull’email principale e su un account finanziario.

☐ TASK 02

Install pending updates and remove one unnecessary browser extension.

Installa gli aggiornamenti e rimuovi un’estensione inutile.

☐ TASK 03

Verify one independent backup and save recovery codes safely.

Verifica un backup indipendente e conserva i codici di recupero.

## What did you change? / Che cosa hai modificato?

_____

_____

_____

Next review date / Prossimo controllo: _____