SYNERGY

powered by SYN Group Inc.

CYBERSECURITY FUNDAMENTALS

A Six-Hour Independent Online Educational Course

PERSONAL • DIGITAL • SMALL-BUSINESS SECURITY

Learn to recognize common cyber risks, protect accounts and devices, safeguard information, and respond more thoughtfully when something goes wrong.

SELF-PACED • SIX LEARNING MODULES • FINAL KNOWLEDGE ASSESSMENT

Course provider: Synergy powered by SYN Group Inc.

Course version: 1.0 | Published: November 2026

Welcome and course overview

Welcome to Synergy Cybersecurity Fundamentals. This independent educational course is designed for adults, consumers, entrepreneurs, and small-business personnel who want a practical introduction to everyday cybersecurity. It focuses on awareness and sensible defensive habits—not advanced technical operations.

Cybersecurity is the practice of protecting devices, accounts, networks, systems, and information from unauthorized access, disruption, misuse, or damage. It is not a one-time setup. Technology, business processes, and threats change, so good security requires ongoing attention.

What you should be able to do by the end

- Explain common cybersecurity terms and why confidentiality, integrity, and availability matter.
- Recognize common phishing, impersonation, payment-diversion, and social-engineering warning signs.
- Choose stronger authentication practices and reduce account-takeover risk.
- Apply basic device, home-network, mobile-device, and software-update precautions.
- Handle business and personal information more carefully, including sharing, storage, retention, and disposal.
- Describe basic preparation, reporting, containment, recovery, and follow-up steps after a suspected incident.

Six-hour course structure

Module	Topic	Time
1	Cybersecurity foundations and risk awareness	60 min
2	Threats, phishing, scams, and social engineering	60 min
3	Passwords, identity, and account protection	60 min
4	Devices, networks, software, and safe browsing	60 min
5	Data protection, privacy, and small-business practices	60 min
6	Incident response, recovery, and final assessment	60 min
	TOTAL SUGGESTED LEARNING TIME	**6 hours**

How the time works: The six-hour duration is the course's suggested instructional workload, including reading, reflection, practical activities, and assessment. Participants should work through all material and activities rather than treating the time estimate as a guaranteed measure of individual learning.

Important scope and safety notice

This is general educational information. It is not a technical security audit, managed security service, legal opinion, compliance assessment, or individualized IT recommendation. Do not test systems, accounts, networks, or devices unless you own them or have clear written authorization. Never use course concepts to access another person's information or bypass security controls.

How to complete the course

1. Read all six modules and their examples.
2. Complete each practical activity using only your own accounts, devices, or a safe hypothetical scenario.
3. Answer the module knowledge checks and complete the final assessment.
4. Review your answers and identify topics you need to study further.
5. At the end, use the certificate request instructions to submit your name and email address to Synergy.

MODULE 1 — Cybersecurity Foundations and Risk Awareness

Suggested learning time: 60 minutes

Cybersecurity begins with understanding what needs protection and what could go wrong. A person does not need to be a programmer to make safer decisions. Awareness, preparation, and consistent habits reduce many everyday risks.

1.1 The three security goals

Confidentiality means information is available only to people or systems that are authorized to see it. Examples include protecting customer records, private messages, and account credentials.

Integrity means information remains accurate and is not changed improperly. A changed invoice bank account, altered customer record, or tampered file can cause real harm.

Availability means systems and information are accessible when legitimately needed. Ransomware, equipment failure, outages, and accidental deletion can interrupt availability.

These goals can conflict. A business may restrict access to protect confidentiality, but it must still ensure authorized staff can perform their work. Security is about managing risk—not making systems unusable.

1.2 Understand assets, threats, vulnerabilities, and risk

An **asset** is something valuable: a phone, laptop, email account, customer list, payment records, website, cloud storage, or business reputation.

A **threat** is something that could cause harm, such as a criminal, malicious software, a dishonest insider, a lost device, a mistake, or a natural event.

A **vulnerability** is a weakness that could be exploited, such as an unpatched application, reused password, exposed admin account, or unlocked phone.

Risk combines the likelihood of a harmful event with its possible impact. A small business should prioritize risks that could cause serious financial, operational, privacy, or reputational damage.

1.3 A practical risk example

Imagine a small company uses one shared email account for invoices, customer conversations, and password resets. If the password is reused on another website and that website is breached, an attacker may try the same password on the company email. If successful, the attacker could read private messages, impersonate the company, or request fraudulent payments.

The weakness is not merely the password. The risk is increased by shared access, password reuse, lack of multifactor authentication, and the account's importance to other services. Controls should address the whole situation.

1.4 A simple risk-prioritization method

List the asset, describe the threat, identify the weakness, estimate the likely impact, and choose a practical control. Consider both likelihood and impact. A rare event with catastrophic consequences may still deserve attention.

Do not assume that a small company is too small to be targeted. Criminals often use automated tools and broad campaigns. A business may be targeted because it has money, customer information, access to another company, or simply an exposed account.

1.5 Security is shared responsibility

Owners set expectations and fund reasonable safeguards. Employees and contractors follow procedures and report suspicious events. Technology providers maintain their own services, but using a provider does not remove every responsibility from the customer.

Use unique user accounts where possible. Avoid sharing passwords. Remove access when a worker or contractor no longer needs it. Review who can access sensitive systems periodically.

Practical learning activity

Choose one personal or business asset, such as your primary email account. Write down: (1) why it matters, (2) one threat, (3) one weakness, (4) the likely impact if compromised, and (5) one control that would reduce the risk.

Now repeat the exercise for a phone, customer file, payment account, or website. Compare which risk would cause the greatest harm and should be addressed first.

Module knowledge check

1. Which statement best describes confidentiality?

A. Information is available only to authorized people or systems.

B. Information is always online.

C. Information can never be copied.

D. Information is backed up every hour.

2. What is a vulnerability?

A. A security weakness that could be exploited.

B. A type of insurance.

C. A confirmed criminal conviction.

D. A software warranty.

3. Which is an example of an asset?

A. A customer database.

B. A phishing attempt.

C. A software flaw.

D. A power outage.

4. Why should a small business assess risk?

A. Only large corporations face cyber threats.

B. Risk assessment helps prioritize protections based on likelihood and impact.

C. It guarantees no incidents will occur.

D. It replaces all security tools.

MODULE 2 — Threats, Phishing, Scams, and Social Engineering

Suggested learning time: 60 minutes

Many cyber incidents begin with a message or conversation that persuades someone to take an unsafe action. Social engineering targets human judgment and routine business processes, not just computer software.

2.1 Phishing and related attacks

Phishing is a deceptive message designed to trick a person into revealing information, opening a harmful attachment, visiting a fraudulent website, or sending money. It may arrive by email, text, social media, or messaging app.

Spear phishing is tailored to a particular person or organization. The message may use a real name, job title, vendor, recent purchase, or public information to appear credible.

Smishing is phishing by text message. **Vishing** is voice-based deception, often through a phone call. **Business email compromise** involves impersonation or compromise of business email to redirect payments, obtain sensitive data, or manipulate transactions.

2.2 Warning signs

Be cautious when a message creates urgency, threatens account closure, promises an unexpected refund, demands secrecy, requests a password or verification code, or asks you to change payment instructions.

Look carefully at the full sender address and domain. A familiar display name does not prove the sender is genuine. A domain can contain extra words, misspellings, or characters that look similar to the real name.

Unexpected attachments, QR codes, shortened links, unusual file types, poor context, and requests to bypass normal procedures deserve extra scrutiny. Professional spelling and logos do not prove authenticity; scammers can produce polished messages.

2.3 Verify through a separate trusted channel

If a vendor emails new bank instructions, do not use the phone number or link in that email to verify the change. Use a phone number already on file or a trusted contact method obtained independently.

If a manager requests an urgent wire transfer or gift cards, pause and confirm through a second channel. Establish a rule that payment-detail changes require independent verification and approval by an authorized person.

Never share one-time passcodes, authenticator approvals, recovery codes, or passwords with someone who contacts you unexpectedly. Legitimate support staff should not need you to disclose your password.

2.4 Malware and ransomware

Malware is software designed to perform harmful or unauthorized actions. It may steal information, spy on activity, disrupt devices, or provide unauthorized access.

Ransomware is malware that blocks access to data or systems, often by encrypting files, and demands payment. Paying does not guarantee recovery or prevent data exposure.

Malware can arrive through malicious attachments, fake software updates, compromised websites, unsafe downloads, removable media, or exploited software vulnerabilities. Use reputable software sources and keep systems updated.

2.5 Deepfakes and AI-enabled deception

AI tools can generate convincing text, voices, images, and video. A familiar voice or realistic video call should not be treated as proof of identity, especially when money, credentials, or sensitive information are requested.

Use agreed verification phrases or callback procedures for high-risk requests. Confirm unusual instructions with a known contact using a different communication channel. Do not rely on a voice alone.

2.6 Safe response to a suspicious message

Do not click, reply, download, scan, or forward the suspicious content casually. Report it through your organization's approved process or the service provider's reporting feature.

If you clicked or entered information, act promptly. From a trusted device, change the affected password, revoke active sessions where available, enable stronger authentication, and contact the relevant bank or provider if financial information may be exposed.

Practical learning activity

Read this scenario: A supplier emails that its bank account has changed and says payment must be sent within two hours. The email includes a new account number and a mobile number for questions. Write down three reasons to pause and the independent steps you would use to verify the request.

Second scenario: A caller claims to be technical support and asks you to read a six-digit login code. Write the sentence you would use to refuse and end the call safely.

Module knowledge check

1. What is the safest way to verify a vendor's unexpected bank-account change?

A. Reply to the email and ask if it is real.

B. Call a trusted number already on file, independent of the message.

C. Use the phone number in the suspicious email.

D. Send a small test payment without verification.

2. What is smishing?

A. Phishing by text message.

B. A type of backup.

C. A secure login method.

D. A software update.

3. A person claiming to be support asks for your one-time code. What should you do?

A. Share it if they know your name.

B. Read it only if the caller sounds professional.

C. Do not share it; independently contact the provider if needed.

D. Post it in a support forum.

4. Why can an AI-generated voice message be risky?

A. AI voices cannot imitate people.

B. A convincing voice is not reliable proof of identity.

C. Voice messages are always encrypted.

D. It means the caller is authorized.

MODULE 3 — Passwords, Identity, and Account Protection

Suggested learning time: 60 minutes

Accounts are gateways to personal and business information. Protecting the email account used for password resets is especially important because access to that inbox may allow an attacker to take over other services.

3.1 Strong, unique passwords and passphrases

Use a different password for every important account. Reusing a password allows a breach at one service to endanger other accounts. A long, unique passphrase can be easier to remember and harder to guess than a short, predictable password.

Avoid names, birthdays, sports teams, common phrases, keyboard patterns, and small variations of an old password. Do not use a password from a data breach again.

A reputable password manager can create and store unique passwords. Protect the password manager itself with a strong master passphrase and multifactor authentication where available. Secure its recovery method.

3.2 Multifactor authentication

Multifactor authentication (MFA) requires more than one type of proof to sign in. Factors may include something you know (a password), something you have (a security key or authenticator device), or something you are (a biometric characteristic).

MFA can reduce the risk of account takeover, especially when a password is stolen. Prefer phishing-resistant options such as passkeys or hardware security keys when a service supports them. Authenticator apps are generally preferable to SMS codes where stronger options are available.

Never approve an unexpected login prompt. Repeated prompts may be an attempt to pressure you into approving an attack. Deny the request and investigate.

3.3 Protect account recovery

Recovery email addresses, phone numbers, backup codes, and trusted devices can be used to regain access. Keep them current and protect them as carefully as the account itself.

Store recovery codes securely and separately from the device or account they protect. Do not send recovery codes to yourself in an ordinary message or leave them visible near a computer.

Review account sessions, devices, connected applications, forwarding rules, and recovery settings. Remove anything you do not recognize. Be cautious: some legitimate services show unfamiliar device names or approximate locations, so verify before taking action.

3.4 Email account security

Use a unique password and MFA for your primary email. Review forwarding rules and filters that might silently copy messages to an unknown address. Check recovery options and active sessions after any suspected compromise.

Be alert for unexpected password-reset messages. Do not follow links in unsolicited notices. Open the provider's official app or type its known website address yourself.

3.5 Identity theft and account takeover

Account takeover occurs when someone gains control of an account without permission. Warning signs can include unfamiliar login alerts, password-reset notices you did not request, messages you did not send, changed recovery details, or transactions you do not recognize.

If you suspect identity theft, secure the affected accounts from a trusted device, contact the service provider, and consider appropriate identity-protection steps. In the United States, IdentityTheft.gov provides recovery guidance for identity theft.

3.6 Least privilege

Use standard accounts for ordinary work and reserve administrator privileges for tasks that truly require them. Do not give every worker access to every customer file or financial system.

Separate personal and business accounts where practical. Review access when roles change and promptly disable accounts that are no longer needed.

Practical learning activity

Create a checklist for your five most important accounts. For each, record whether its password is unique, MFA is enabled, recovery details are current, and active sessions are reviewed. Do not write the actual passwords in this course workbook.

Identify which account could be used to reset the others. Give that account priority for a unique password, strong MFA, and secure recovery settings.

Module knowledge check

1. Why should passwords be unique across services?

A. It prevents a breach at one service from automatically exposing reused credentials elsewhere.

B. It makes passwords public.

C. It eliminates the need for MFA.

D. It guarantees an account cannot be hacked.

2. Which is generally a stronger MFA choice when supported?

A. Approving every unexpected prompt.

B. A phishing-resistant passkey or security key.

C. Reusing an SMS code.

D. Sharing a code with support.

3. What should you do with an unexpected login approval prompt?

A. Approve it to stop the notifications.

B. Ignore all future alerts.

C. Deny it and investigate through the provider's official channel.

D. Send the prompt to a stranger.

4. What does least privilege mean?

A. Everyone receives administrator access.

B. Users receive only the access needed for their role.

C. Passwords are shared by a team.

D. No one can access business files.

MODULE 4 — Devices, Networks, Software, and Safe Browsing

Suggested learning time: 60 minutes

Phones, computers, routers, browsers, and cloud-connected devices all contribute to cybersecurity. A secure account can still be exposed through an outdated or poorly protected device.

4.1 Device basics

Use a strong device passcode or password and enable automatic screen locking. Use biometrics as a convenience layer where appropriate, while retaining a strong passcode. Configure device-finding and remote-wipe features if available.

Keep operating systems, browsers, applications, and firmware current. Updates often fix security weaknesses. Enable automatic updates where appropriate and restart devices when required to complete them.

Install applications only from reputable official sources. Review app permissions and remove applications you no longer use. Be cautious with sideloaded applications, unofficial app stores, and unexpected software downloads.

4.2 Endpoint protection

Endpoint protection includes safeguards on laptops, desktops, phones, and servers. Use reputable built-in or commercial security tools, keep them updated, and do not disable protection because a pop-up or caller tells you to.

Use standard user accounts for routine activity. Restrict administrator access. Lock devices when unattended and avoid leaving sensitive information visible in public places.

Lost devices should be reported quickly. Use the device provider's official tools to lock, locate, or erase a missing device when appropriate. Change credentials that may have been stored or accessible on it.

4.3 Home and small-office Wi-Fi

Change default router administrator credentials. Use modern Wi-Fi security supported by your equipment, such as WPA3 or WPA2-AES, and choose a strong network passphrase. Keep router firmware updated.

Disable features you do not need, such as remote administration from the internet, unless you understand and securely manage them. Use a guest network for visitors and untrusted devices when available.

Do not assume a network is safe simply because it has a password. Public Wi-Fi may be monitored or impersonated. Avoid sensitive activity on networks you do not trust; use the official app or website and appropriate secure connections.

4.4 Browsers and websites

Check the domain name carefully before signing in. HTTPS encrypts the connection between your browser and the site, but it does not prove that the website itself is honest. Scam websites can also use HTTPS.

Type important website addresses yourself or use a trusted bookmark. Be wary of search advertisements or sponsored results that imitate a provider. Avoid entering credentials after following an unexpected message link.

Browser extensions can read or change information on websites depending on their permissions. Install only extensions you need from trusted publishers, review permissions, and remove unused extensions.

4.5 Backups and recovery

Backups protect against accidental deletion, hardware failure, ransomware, and other disruptions. Identify important data and back it up regularly according to how often it changes and how much loss the business can tolerate.

Keep at least one backup protected from routine access by compromised systems. Offline or otherwise isolated backups can reduce the chance that ransomware affects both production data and backups.

A backup is not proven useful until restoration has been tested. Periodically restore sample files or systems and document who is responsible, where backups are stored, and how recovery works.

4.6 Cloud services and connected devices

Cloud storage and software services can improve collaboration but must be configured carefully. Review sharing links, public access settings, user permissions, and external collaborators.

Smart cameras, printers, voice assistants, point-of-sale devices, and other connected equipment can introduce risk. Change default credentials, install updates, limit network access, and retire devices that no longer receive security support.

Practical learning activity

Perform a safe personal-device review: check for pending operating-system updates, remove one unused app, review app permissions, confirm a screen lock is enabled, and verify that device-finding or backup settings are configured as you intend.

Do not scan networks or attempt to access devices that are not yours. For a router you own or administer, review the manufacturer's official instructions before changing settings.

Module knowledge check

1. Does HTTPS prove a website is legitimate?

A. Yes, always.

B. No. It protects the connection but does not prove the site is trustworthy.

C. Only on phones.

D. Only when the page has a logo.

2. Why test backups?

A. To confirm that data can actually be restored.

B. To make files public.

C. To remove the need for updates.

D. To guarantee zero downtime.

3. What is a sensible router practice?

A. Keep the factory administrator password forever.

B. Change default credentials and install firmware updates.

C. Share the admin password publicly.

D. Disable all security settings.

4. What should you do before installing an unexpected software update from a pop-up?

A. Click immediately.

B. Call the number shown in the pop-up.

C. Close it and obtain updates through the device or software's official update mechanism.

D. Download a remote-access tool.

MODULE 5 — Data Protection, Privacy, and Small-Business Practices

Suggested learning time: 60 minutes

Information is often a business's most valuable and most sensitive asset. A small organization can improve its security by knowing what information it collects, limiting who can access it, sharing it carefully, and disposing of it when no longer needed.

5.1 Know what information you hold

Create a simple inventory of important information: customer contact details, identification documents, payment information, employee records, contracts, credentials, business plans, and backups.

Understand where information is stored and how it moves: email, phones, laptops, cloud drives, paper files, payment systems, websites, and service providers. Unknown copies and forgotten accounts can create unnecessary exposure.

Collect only information that has a legitimate business purpose. Avoid collecting sensitive information simply because a form makes it easy. Less data generally means less data to protect.

5.2 Classify and limit access

Use practical categories such as public, internal, confidential, and highly sensitive. The labels should help people decide how to store, share, and dispose of information.

Apply least privilege. Give people access only to the information needed for their responsibilities. Use separate accounts rather than shared logins, and remove access when it is no longer required.

Do not send sensitive information through ordinary unprotected channels just because it is convenient. Use approved secure portals or encrypted sharing methods where appropriate. Verify recipients before sending.

5.3 Secure sharing and remote work

Before sharing a cloud document, confirm the recipient, access level, expiration date, and whether downloading or resharing should be allowed. Avoid public links for confidential documents.

Use approved business devices and accounts where practical. Protect home workspaces, lock screens, and avoid discussing confidential matters where others can overhear.

Be cautious when using public computers or shared devices. Do not save passwords, leave accounts signed in, or download sensitive business files to devices you do not control.

5.4 Vendors and third parties

Payroll providers, cloud storage companies, payment processors, website hosts, consultants, and software vendors may handle business information. Before relying on a provider, understand what information it receives, how it protects it, how incidents are reported, and how data is returned or deleted when the relationship ends.

Use written agreements that address confidentiality, access, security expectations, incident notification, and data handling where appropriate. Do not assume a vendor's marketing statement answers every security question.

Limit vendor access to what is needed and review it periodically. Use separate accounts and revoke access when work is complete.

5.5 Retention and secure disposal

Keep information only as long as there is a legitimate business, legal, or operational reason. Retention requirements vary by information type and applicable law, so do not destroy records that must be preserved.

When information is no longer needed, dispose of it securely. Shred sensitive paper records and use appropriate secure deletion or device disposal processes. Simply moving a file to a recycle bin may not securely erase it.

Have a clear process for handling old devices, removable drives, printed records, and former employee accounts.

5.6 Policies and human behavior

Even a small business benefits from short written rules covering passwords, MFA, acceptable device use, data sharing, payment verification, backups, remote work, incident reporting, and employee departures.

Train people using realistic examples. Encourage prompt reporting of mistakes without creating a culture where people hide incidents out of embarrassment. Early reporting can reduce harm.

Legal, regulatory, contractual, and industry requirements depend on the type of business and information involved. A general course cannot determine which requirements apply to every participant. Obtain qualified advice when necessary.

Practical learning activity

Create a one-page information-handling plan for a hypothetical small business. List three types of information it holds, where each is stored, who needs access, how it is shared, and when it should be reviewed or securely disposed of.

Write a payment-change verification rule in one sentence. Example: 'Any request to change payment instructions must be verified by calling a previously recorded trusted number, with a second authorized person approving the change.'

Module knowledge check

1. What is data minimization?

A. Collecting and keeping only information needed for a legitimate purpose.

B. Saving every document forever.

C. Giving all employees access to all files.

D. Sending all data to every vendor.

2. What is least privilege applied to data?

A. Everyone can read every file.

B. Access is limited to what a person needs for their role.

C. Only managers use passwords.

D. Customer records are posted publicly.

3. How should a business verify changed payment instructions?

A. Use the phone number in the change email.

B. Verify independently using a trusted contact method already on file.

C. Assume the email account is genuine.

D. Pay quickly to avoid a late fee.

4. Why review third-party vendors?

A. They may access or process business information and create additional risk.

B. Vendors never create security risk.

C. It removes the need for internal controls.

D. It guarantees a vendor will never be breached.

MODULE 6 — Incident Response, Recovery, and Final Assessment

Suggested learning time: 60 minutes

Even organizations with good safeguards can experience incidents. A prepared, calm, documented response can limit damage. The right response depends on what happened, which systems are affected, and the organization's legal and contractual duties.

6.1 Recognize and report an incident

A security incident may include a lost device, suspicious login, malware alert, unauthorized account access, exposed document, misdirected email, fraudulent payment request, or unexpected change to business data.

Report suspected incidents promptly through the organization's designated contact or service provider. Include what happened, when it was noticed, which device or account is involved, and what actions have already been taken.

Do not delete messages, wipe devices, or conduct your own intrusive investigation before getting appropriate guidance. Preserve relevant evidence where safe and practical.

6.2 Contain safely

Containment aims to prevent further harm. Depending on the situation, this may mean disconnecting a compromised device from networks, disabling a compromised account, revoking active sessions, blocking a fraudulent payment, or contacting a provider.

Do not turn off or alter a device if doing so could destroy important evidence or conflict with an incident-response plan. Follow instructions from qualified responders, IT staff, or the relevant provider.

If financial information may be exposed, contact the bank or payment provider promptly using a trusted number. Ask about securing the account, stopping or disputing transactions, and preserving records.

6.3 Recover and restore

Recovery may involve resetting credentials, rebuilding devices, restoring clean backups, patching weaknesses, validating systems, and carefully returning services to operation.

Do not restore from a backup until you have reasonable confidence it is clean and the underlying weakness has been addressed. Test restored data and monitor accounts and systems for signs of continued access.

Recovery priorities should be based on business impact. Identify which services are essential, who can authorize restoration, and how customers or partners will be informed.

6.4 Notification and documentation

Document the timeline, affected systems, decisions, contacts, actions, and costs. Accurate records help with investigation, recovery, insurance, and required notifications.

Notification duties depend on the type of information, location, industry, contracts, and applicable law. Do not assume one universal deadline or rule applies. Consult legal counsel, regulators, insurers, and relevant providers as appropriate.

Communicate carefully. Avoid speculation, unsupported assurances, or statements that an incident is resolved before that has been confirmed.

6.5 Learn and improve

After the immediate response, identify how the incident began, which controls failed or were missing, what worked, and what should change. Update training, access controls, vendor requirements, backups, and procedures.

Use the NIST Cybersecurity Framework 2.0 as one voluntary risk-management reference. Its functions are Govern, Identify, Protect, Detect, Respond, and Recover. The framework is flexible and is not a guarantee of security or a certification earned by reading this course.

Cybersecurity is continuous. Schedule periodic reviews of important accounts, software, devices, access permissions, vendors, and backup restoration.

6.6 Personal action plan

Choose three improvements you can realistically complete: for example, enable MFA on your primary email, replace a reused password, update a router, review cloud sharing, or test a backup.

Assign an owner and target date to each action. Revisit the list after completion and whenever important systems, staff, vendors, or risks change.

Practical learning activity

Draft a simple incident contact sheet for a hypothetical business. Include the owner or incident lead, IT support, bank/payment provider, insurance contact, legal contact, and critical technology vendors. Use official contact information already on file; do not invent phone numbers.

Write a five-step response plan: report, assess, contain, recover, and review. Identify who is authorized to make decisions and how records will be preserved.

Module knowledge check

1. What should happen when a suspected incident is discovered?

A. Hide it until certain.

B. Report it promptly through the designated process and preserve relevant details.

C. Delete all messages immediately.

D. Post passwords online to warn others.

2. What is the purpose of containment?

A. Preventing further harm or spread.

B. Making the incident public before facts are known.

C. Deleting every backup.

D. Guaranteeing no data was exposed.

3. What should be considered before restoring a backup?

A. Whether the backup is clean and the underlying weakness has been addressed.

B. Whether the backup is the oldest available.

C. Whether the password is shared.

D. Whether the device has a familiar name.

4. What is the NIST CSF 2.0 function set?

A. Govern, Identify, Protect, Detect, Respond, Recover.

B. Buy, Sell, Market, Advertise, Hire, Retire.

C. Scan, Exploit, Hide, Delete, Transfer, Repeat.

D. Install, Print, Email, Call, Text, Sign.

FINAL KNOWLEDGE ASSESSMENT

Complete this assessment after reviewing all six modules. Select one best answer for each question. A suggested passing standard for this independent course is 16 correct answers out of 20 (80%). Synergy may review or adjust the assessment and passing standard as part of course administration.

1. Which three goals are commonly used to describe information security?

A. Confidentiality, integrity, availability

B. Speed, cost, convenience

C. Privacy, marketing, sales

D. Hardware, software, support

2. A weakness in a system that could be exploited is called:

A. An asset

B. A vulnerability

C. A backup

D. A certificate

3. A message creates urgency and asks you to sign in through an unfamiliar link. The safest response is:

A. Click quickly

B. Reply with your password

C. Avoid the link and verify through the service's official channel

D. Forward it to everyone

4. A supplier emails new bank instructions. You should:

A. Use the number in the email

B. Independently call a trusted number already on file

C. Assume it is valid if the logo is correct

D. Send a small payment first

5. A one-time login code should be:

A. Shared with anyone claiming to be support

B. Posted in a ticket

C. Kept private and never disclosed to an unexpected caller

D. Used as a permanent password

6. Why use unique passwords?

A. To reduce the impact of a password breach at another service

B. To avoid updates

C. To replace backups

D. To make passwords easier to guess

7. Which option is generally more resistant to phishing when supported?

A. A passkey or security key

B. A code sent to a stranger

C. A reused password

D. An unexpected login approval

8. Least privilege means:

A. Everyone is an administrator

B. Access is limited to what is needed

C. All files are public

D. Accounts are shared

9. HTTPS means:

A. The site is guaranteed legitimate

B. The connection is encrypted, but the site may still be fraudulent

C. The site is government-approved

D. The device has no malware

10. Why update software?

A. Updates can fix known security weaknesses

B. Updates guarantee no incidents

C. Updates replace MFA

D. Updates make backups unnecessary

11. A good backup practice includes:

A. Never testing it

B. Keeping all copies connected and writable

C. Testing restoration and protecting a backup from routine compromise

D. Saving only one copy on the same device

12. A router should generally have:

A. Default admin credentials

B. Updated firmware and changed default credentials

C. An openly shared admin password

D. No encryption

13. Data minimization means:

A. Keeping all data forever

B. Collecting and retaining only what is needed for a legitimate purpose

C. Sending data to every vendor

D. Giving everyone access

14. Before sharing a confidential cloud document, check:

A. Recipient and access permissions

B. Only the document color

C. Whether the link is short

D. Whether the file name is interesting

15. A vendor's security should be considered because:

A. Vendors may access or process your information

B. Vendors never experience incidents

C. It removes all business risk

D. It means you do not need policies

16. If you suspect an account compromise, you should:

A. Ignore it

B. Use a trusted device and official provider channels to secure the account

C. Send your password to the caller

D. Delete all evidence

17. Incident containment is intended to:

A. Limit further harm

B. Guarantee the attacker is identified

C. Replace legal advice

D. Make the issue disappear without records

18. Before restoring data, consider whether:

A. The backup is clean and the weakness has been addressed

B. The backup is the oldest

C. The password is shared

D. The device is online

19. Notification obligations after a breach:

A. Are identical in every situation

B. Depend on facts, applicable laws, contracts, and the type of information

C. Never apply to small businesses

D. Are decided by a social media poll

20. The NIST Cybersecurity Framework 2.0 includes:

A. Govern, Identify, Protect, Detect, Respond, Recover

B. Only Protect and Recover

C. Only passwords and antivirus

D. Six mandatory certifications

Completion reflection and certificate request

Before requesting your certificate, confirm that you have read all six modules, completed the practical activities, and answered the final assessment. Review any incorrect answers and revisit the relevant module.

Personal cybersecurity action plan

1. One account I will secure first: _____

2. One device or application I will update or review: _____

3. One data-sharing or privacy habit I will improve: _____

4. One backup or recovery step I will take: _____

5. The date I plan to review these actions: _____

Requesting your Synergy certificate

After completing the course and final assessment, use the certificate request method provided on the Synergy website. Submit your full name and email address and identify the course as **Cybersecurity Fundamentals — Six-Hour Course**. Synergy will review the request and, if completion requirements are met, send the certificate to the email address provided within the stated processing period.

> **Suggested website instruction:** “Congratulations on completing Synergy Cybersecurity Fundamentals. To request your Certificate of Completion, enter your full name and email address in the fields below and submit your request. Certificate requests are reviewed by Synergy and qualifying certificates are emailed within 48–72 hours.”

The certificate records completion of this independent Synergy educational course. It does not represent a government-issued license, university credit, accreditation, or a third-party professional certification. It does not certify that a participant is qualified to perform cybersecurity work.

Course disclosure

Synergy, powered by SYN Group Inc., provides this course for general educational and informational purposes. The course is independently developed and is not affiliated with, endorsed by, or sponsored by Cisco, any university, government agency, or third-party certification provider. The course is not an accredited educational program and does not provide a professional license or industry-recognized cybersecurity qualification.

Course content is intended to provide introductory awareness and general defensive practices. It is not individualized technical, legal, compliance, or professional security advice; it is not a security audit or guarantee that any device, account, network, or organization is secure. Participants should consult qualified professionals for needs specific to their circumstances.

Cybersecurity technologies, threats, recommendations, and applicable requirements change over time. Content should be reviewed periodically and may become outdated. No particular result, employment opportunity, level of technical skill, or protection from cyber incidents is guaranteed. Participants must use all information lawfully and only on systems they own or are authorized to administer.

References and further learning

This course is independently written and uses publicly available guidance as reference material. Participants are encouraged to consult current primary sources because guidance may change:

- **National Institute of Standards and Technology (NIST):** Cybersecurity Framework 2.0 and Small Business Quick-Start Guide — https://www.nist.gov/publications/nist-cybersecurity-framework-20-small-business-quick-start-guide
- **NIST:** Cybersecurity Basics for Small Business — https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics
- **Federal Trade Commission (FTC):** Cybersecurity for Small Business — https://www.ftc.gov/business-guidance/small-businesses/cybersecurity
- **FTC:** Protecting Personal Information: A Guide for Business — https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business
- **Federal Bureau of Investigation (FBI):** Cybersecurity Best Practices — https://www.fbi.gov/investigate/cyber/cybersecurity-best-practices
- **Cybersecurity and Infrastructure Security Agency (CISA):** Guidance for small and mid-sized businesses — https://www.cisa.gov/

End of course. Thank you for participating.