IT Cybersecurity Awareness

1. Cybersecurity Awareness

1.1 Intro Slide

Banner Health

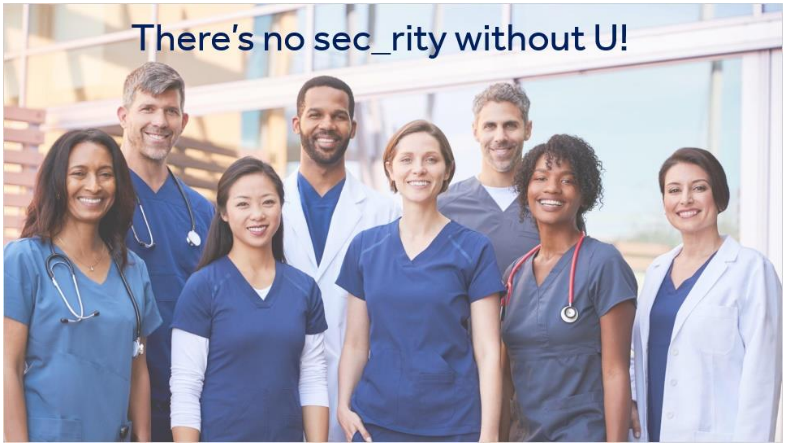
IT Cybersecurity

Awareness Training

Notes:

Welcome to the IT Cybersecurity Awareness Training course.

1.2 Cyber Mission

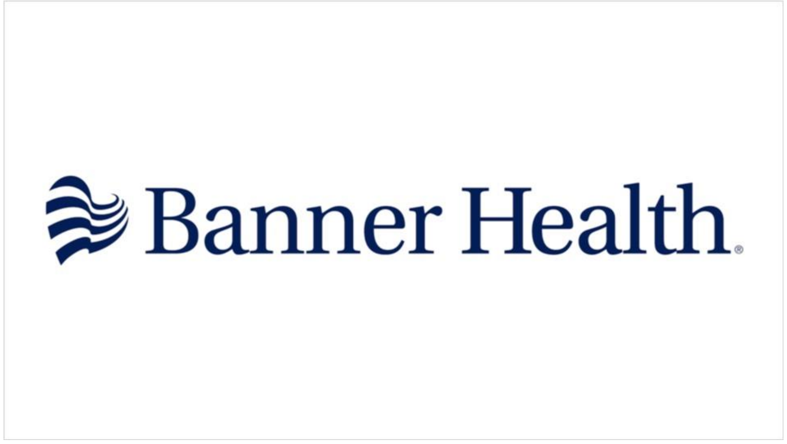


There's no sec_rity without U!

Notes:

At Banner, it takes all of us to help keep our data *and* Sofia safe. While this training is important from a regulatory and compliance perspective, the concepts can also be applied to your life outside of work.

1.3 CISO



Notes:

Hello, my name is Dave Schauble, Chief Information Security Officer for Banner Health.

This education module is designed to inform and remind you of your cybersecurity responsibilities to protect Sofia and Banner.

These principles can also protect you in your personal life.

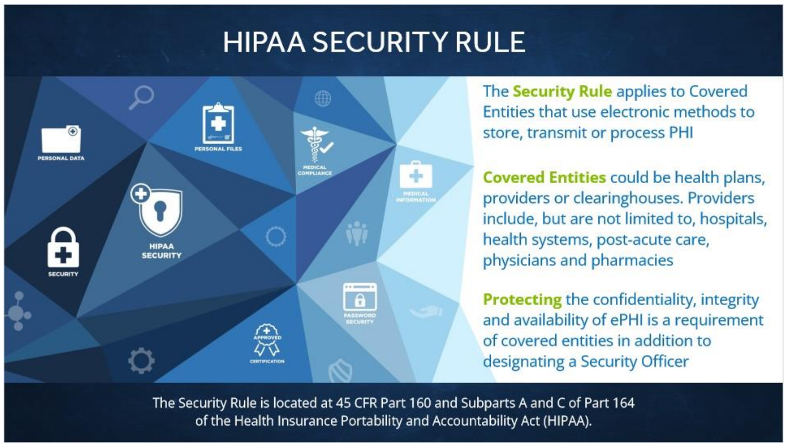
We refresh this information every year to include the most current tactics of cyber criminals and their attacks.

Education and awareness is *the* best protection, and *you* are our first line of defense against these attacks.

Let’s work together to protect our customers, data and each other.

Thank you.

1.4 HIPAA Security Rule 1



HIPAA SECURITY RULE

The **Security Rule** applies to Covered Entities that use electronic methods to store, transmit or process PHI

Covered Entities could be health plans, providers or clearinghouses. Providers include, but are not limited to, hospitals, health systems, post-acute care, physicians and pharmacies

Protecting the confidentiality, integrity and availability of ePHI is a requirement of covered entities in addition to designating a Security Officer

The Security Rule is located at 45 CFR Part 160 and Subparts A and C of Part 164 of the Health Insurance Portability and Accountability Act (HIPAA).

Notes:

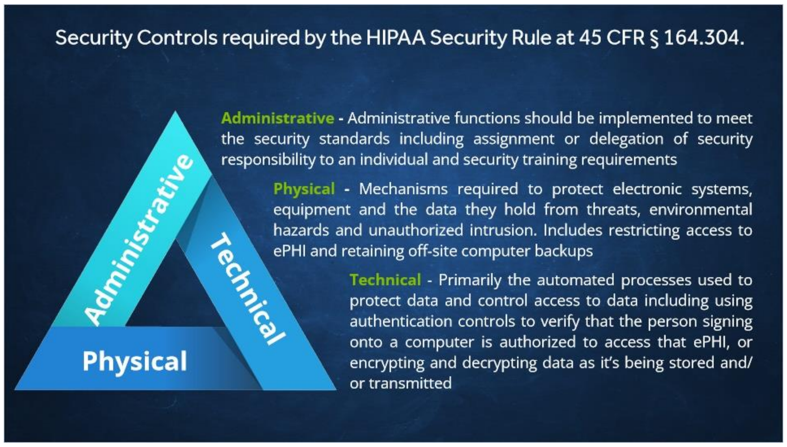
The HIPAA Security Rule requires training to be conducted upon hire and on an annual basis. The Security Rule applies to Covered Entities that use electronic methods to store, transmit or process PHI.

Covered Entities could be health plans, providers or clearinghouses. Providers include, but are not limited to, hospitals, health systems, post-acute care, physicians and pharmacies.

Protecting the confidentiality, integrity and availability of ePHI is a requirement of covered entities in addition to designating a Security Officer.

The Security Rule is located at 45 CFR Part 160 and Subparts A and C of Part 164.

1.5 HIPAA Security Rule 2


Administrative
Technical
Physical

Security Controls required by the HIPAA Security Rule at 45 CFR § 164.304.

Administrative - Administrative functions should be implemented to meet the security standards including assignment or delegation of security responsibility to an individual and security training requirements

Physical - Mechanisms required to protect electronic systems, equipment and the data they hold from threats, environmental hazards and unauthorized intrusion. Includes restricting access to ePHI and retaining off-site computer backups

Technical - Primarily the automated processes used to protect data and control access to data including using authentication controls to verify that the person signing onto a computer is authorized to access that ePHI, or encrypting and decrypting data as it's being stored and/ or transmitted

Notes:

The HIPAA Security Rule requires security controls in three categories:

Administrative - Administrative functions should be implemented to meet the security standards including assignment or delegation of security responsibility to an individual and security training requirements

Physical - Mechanisms required to protect electronic systems, equipment and the data they hold, from threats, environmental hazards and unauthorized intrusion. Includes restricting access to ePHI and retaining off-site computer backups

Technical - Primarily the automated processes used to protect data and control access to data including using authentication controls to verify that the person signing onto a computer is authorized to access that ePHI, or encrypting and decrypting data as it is being stored and/or transmitted

1.6 Course Objectives

COURSE OBJECTIVES

Understand your Cybersecurity responsibilities

Learn the policies to protect our data and Sofia

Review consequences for failing to follow appropriate security policies

Recognize and know how to report cybersecurity incidents

Notes:

This course has four learning objectives. By the end of this course, you should:

- Understand your cybersecurity responsibilities
- Learn the policies to protect our data and Sofia
- Review consequences for failing to follow appropriate security policies
- Recognize and know how to report cybersecurity incidents

1.7 Objective 1

COURSE OBJECTIVES

Understand your Cybersecurity responsibilities

Learn the policies to protect our data and Sofia

Review consequences for failing to follow appropriate security policies

Recognize and know how to report cybersecurity incidents

Notes:

Let’s take a look at the first objective.

1.8 Cybersecurity Responsibilities

Your Cybersecurity Responsibilities

Notes:

We know that cybersecurity is important and everyone has a role to play in ensuring Sofia and our data is safe. It’s important for you to understand your cybersecurity responsibilities.

1.9 Cybersecurity Definition

CYBERSECURITY is the balanced protection of information resources that enables the business to perform its primary functions through the use of tools, policies and standards.

Notes:

Cybersecurity is the balanced protection of information resources that enable the business to perform its primary functions through the use of tools, policies and standards.

1.10 Social Engineering

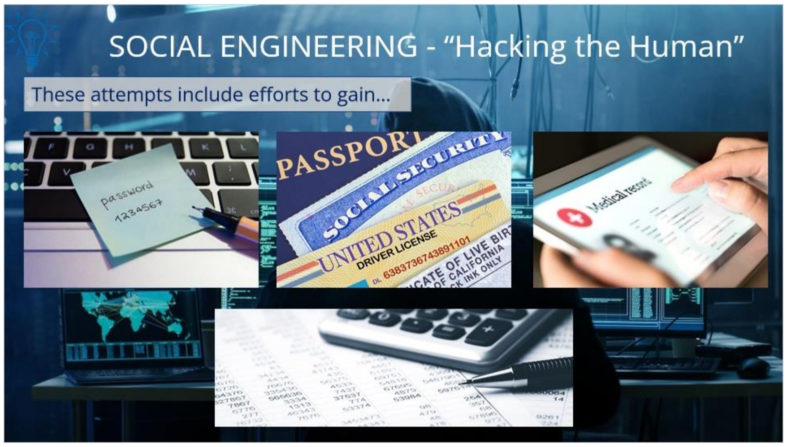
SOCIAL ENGINEERING - “Hacking the Human”

The complex ways cyber criminals trick you into taking actions that benefit their goals

Notes:

One of the major threats we see in Cybersecurity is social engineering, or what we like to refer to as “hacking the human”. Social engineering refers to the complex ways cyber criminals trick you into taking actions that benefit their goals.

1.11 Hacker's goals



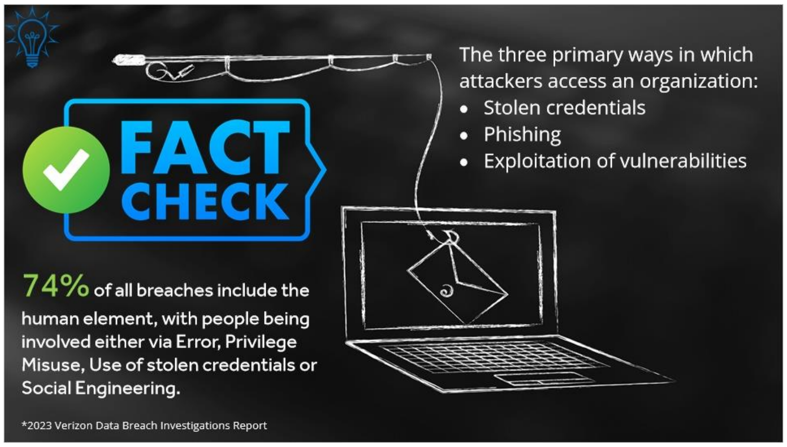
SOCIAL ENGINEERING - “Hacking the Human”

These attempts include efforts to gain...

Notes:

These attempts include efforts to gain: passwords, financial information, personally identifiable information (PII), protected health information (PHI), and more! Some of the ways this is accomplished is through smishing, vishing, and phishing.

1.12 Social Engineering Attacks



The three primary ways in which attackers access an organization:

- Stolen credentials
- Phishing
- Exploitation of vulnerabilities

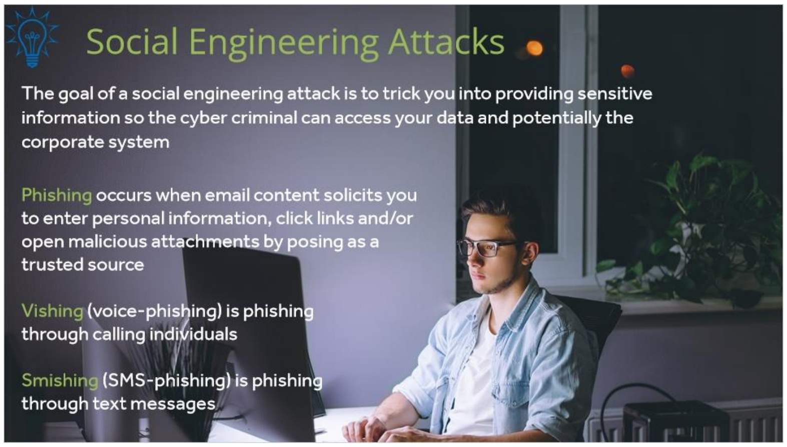
74% of all breaches include the human element, with people being involved either via Error, Privilege Misuse, Use of stolen credentials or Social Engineering.

*2023 Verizon Data Breach Investigations Report

Notes:

From the 2023 Verizon Data Breach Investigations Report, we've learned that 74% of all breaches include the human element, with people being involved either via error, privilege misuse, use of stolen credentials or social engineering. Phishing is still one of the three primary ways in which attackers access an organization, which is why its important to recognize and report any potential phishing attempts.

1.13 Social Engineering Attacks



Social Engineering Attacks

The goal of a social engineering attack is to trick you into providing sensitive information so the cyber criminal can access your data and potentially the corporate system

Phishing occurs when email content solicits you to enter personal information, click links and/or open malicious attachments by posing as a trusted source

Vishing (voice-phishing) is phishing through calling individuals

Smishing (SMS-phishing) is phishing through text messages

Notes:

The goal of a social engineering attack is to trick you into providing sensitive information so the cyber criminal can access your data, and potentially, the corporate system

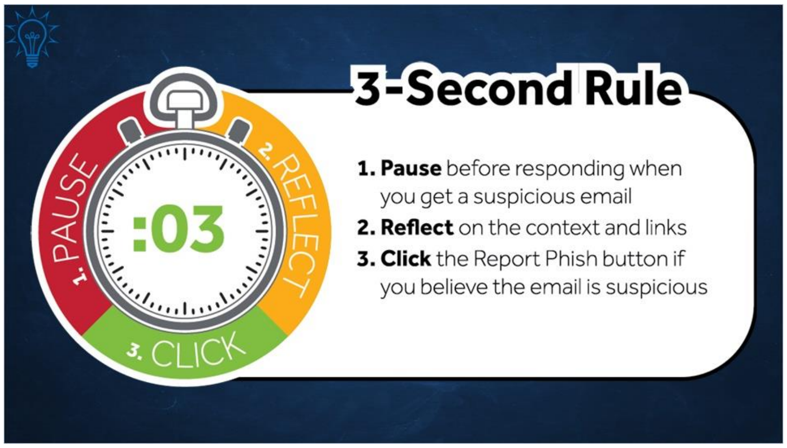
The most common form of social engineering is phishing.

Phishing occurs when email content solicits you to enter personal information, click links, and/or open malicious attachments by posing as a trusted source.

Vishing (voice-phishing) is phishing through calling individuals,

Smishing (SMS-phishing) is phishing through text messages,

1.14 3-Second Rule



3-Second Rule

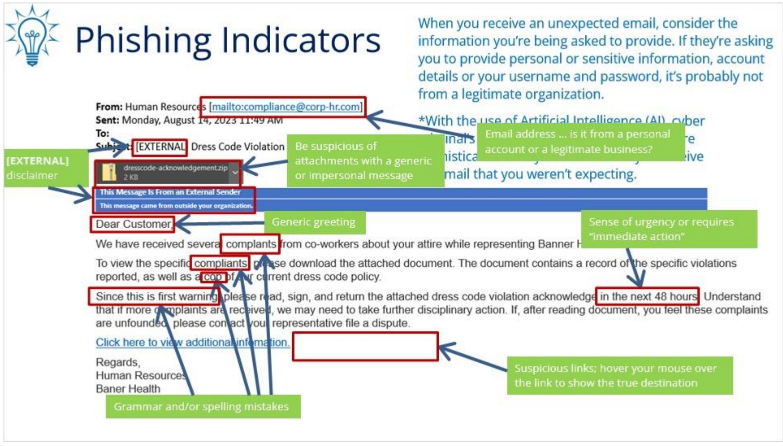
1. **Pause** before responding when you get a suspicious email
2. **Reflect** on the context and links
3. **Click** the Report Phish button if you believe the email is suspicious

Notes:

Before we get into spotting a phishing attempt, let's take a look at the three-second rule. It only takes three seconds to make a difference between clicking and not clicking on a phishing email.

Pause before responding when you get a suspicious email. Make sure to reflect on the context and links. Is this an email you were expecting? And finally click the report phish button located in your Outlook toolbar if you believe the email is a phish.

1.15 Phishing Indicators



Phishing Indicators

When you receive an unexpected email, consider the information you're being asked to provide. If they're asking you to provide personal or sensitive information, account details or your username and password, it's probably not from a legitimate organization.

*With the use of Artificial Intelligence (AI), cyber inal's re istica ive mail that you weren't expecting.

From: Human Resources [mailto:compliance@corp-hr.com]
Sent: Monday, August 14, 2023 11:49 AM
To:
Subject: [EXTERNAL] Dress Code Violation

This Message Is From an External Sender
This message came from outside your organization.

Dear Customer

We have received several complants from co-workers about your attire while representing Banner H

To view the specific compliants, please download the attached document. The document contains a record of the specific violations reported, as well as a cop of our current dress code policy.

Since this is first warning, please read, sign, and return the attached dress code violation acknowledge in the next 48 hours. Understand that if more complaints are received, we may need to take further disciplinary action. If, after reading document, you feel these complaints are unfounded, please contact your representative file a dispute.

Click here to view additional information.

Regards,
Human Resources
Baner Health

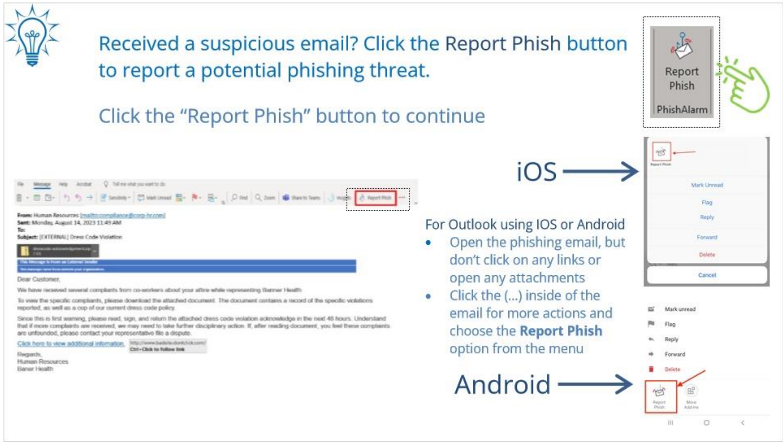
dresscode-acknowledgement.zip
2 KB
[EXTERNAL] disclaimer
Email address ... is it from a personal account or a legitimate business?
Be suspicious of attachments with a generic or impersonal message
Generic greeting
Sense of urgency or requires "immediate action"
Suspicious links; hover your mouse over the link to show the true destination
Grammar and/or spelling mistakes

Notes:

There are seven indicators that you can look for when you receive a suspicious email

- [EXTERNAL] disclaimer
- Email address … is it from a personal account or a legitimate business?
- Generic greeting … "Dear Customer"
- Grammar or spelling mistakes
- Sense of urgency or requires "immediate action"
- Suspicious links; hover your mouse over the link to show the true destination
- Be suspicious of attachments with a generic or impersonal message
- When you receive an unexpected email, consider the information you're being asked to provide. If they're asking you to provide personal or sensitive information, account details or your username and password, it's probably not from a legitimate organization.
- With the use of Artificial Intelligence (AI), cyber criminal's phishing emails are becoming more sophisticated. Always be cautious if you receive an email that you weren't expecting.

1.16 Report Phish



Received a suspicious email? Click the Report Phish button to report a potential phishing threat.

Click the "Report Phish" button to continue

From: Human Resources [mailto:compliance@corp-hr.com]
Sent: Monday, August 14, 2023 11:49 AM
To:
Subject: [EXTERNAL] Dress Code Violation

This Message Is From an External Sender
This message came from outside your organization.

Dear Customer,

We have received several complaints from co-workers about your attire while representing Banner Health.

To view the specific complaints, please download the attached document. The document contains a record of the specific violations reported, as well as a cop of our current dress code policy.

Since this is first warning, please read, sign, and return the attached dress code violation acknowledge in the next 48 hours. Understand that if more complaints are received, we may need to take further disciplinary action. If, after reading document, you feel these complaints are unfounded, please contact your representative file a dispute.

Click here to view additional information. http://www.badsite.dontclick.com/ Ctrl+Click to follow link

Regards,
Human Resources
Baner Health

For Outlook using IOS or Android

- Open the phishing email, but don't click on any links or open any attachments
- Click the (...) inside of the email for more actions and choose the **Report Phish** option from the menu

Notes:

If you *do* receive an email that you think might be suspicious, please click the Report Phish button in the upper right corner of your Outlook toolbar.

For Outlook using IOS or Android

Open the phishing email, but don't click on any links or open any attachments

Click the (...) inside of the email for more actions and choose the **Report Phish** option from the menu

Click the "Report Phish" button to proceed

1.17 Password Best Practices

Password Best Practices

Don't write your passwords down.

Use passphrases instead of passwords.

Use a different password at work than you use for your social media accounts.

Don't share your passwords with your team members.

Check emails before forwarding to ensure no login information is in the email string.

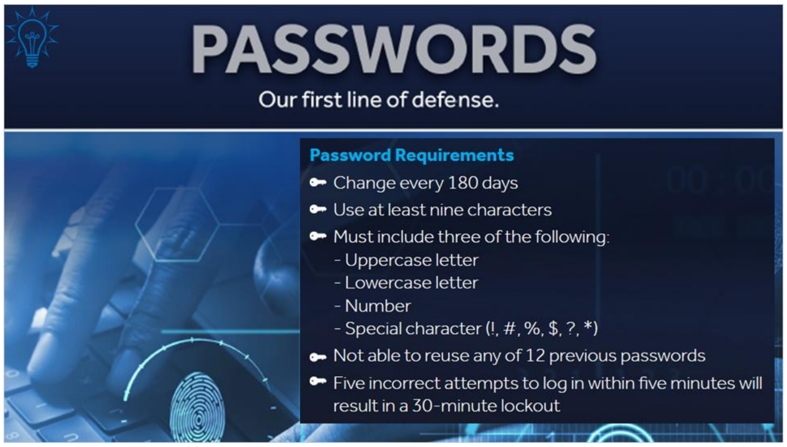
If you suspect that there have been unauthorized access attempts on your account(s), contact the Service Desk.

Notes:

Another important part of your cybersecurity responsibility is password management. There are a few easy things you can do to help ensure your passwords are more secure.

Don’t write your passwords down.
Try using a passphrase instead of passwords.
Use a different password at work than you use for your social media accounts.
Don’t share your passwords with team members.
Remember to check emails before forwarding to ensure no login information is in the email string.
If you suspect that there have been unauthorized access attempts on your account(s), contact the Service Desk.

1.18 Password Best Practices



PASSWORDS

Our first line of defense.

Password Requirements

- Change every 180 days
- Use at least nine characters
- Must include three of the following:
  - Uppercase letter
  - Lowercase letter
  - Number
  - Special character (!, #, %, $, ?, *)
- Not able to reuse any of 12 previous passwords
- Five incorrect attempts to log in within five minutes will result in a 30-minute lockout

Notes:

Passwords are our first line of defense.

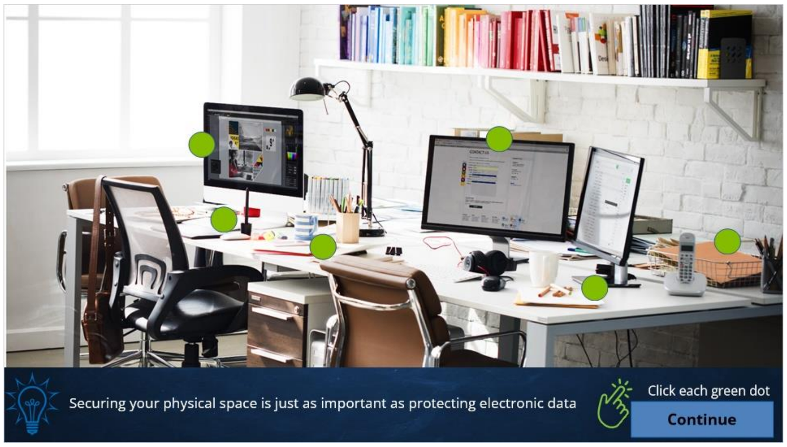
Banner requirements for passwords are:

You must change it every 180 days
You must use at least nine characters
It must include three of the following:

Uppercase letter
Lowercase letter
Number
Special characters.

You aren’t able to reuse any of your 12 previous passwords
Five incorrect attempts to log in within five minutes will result in a 30 minute lockout

1.19 Physical Cybersecurity



Securing your physical space is just as important as protecting electronic data

Click each green dot

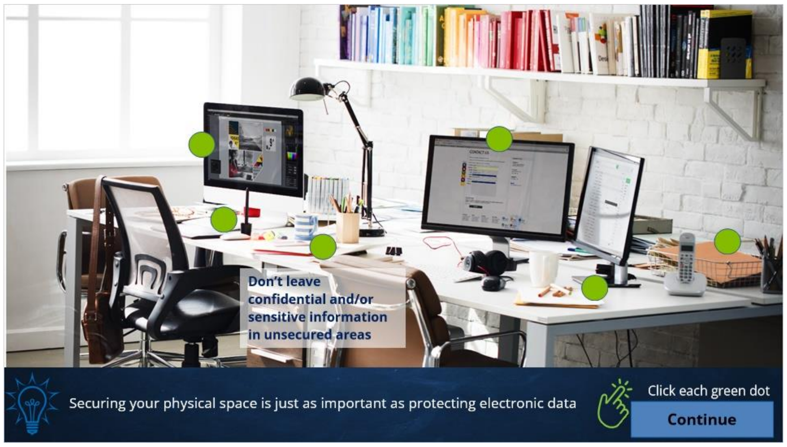
Notes:

Securing your physical space is just as important as protecting electronic data.

Click each green dot to learn more:

- Do not leave confidential and restricted information in unsecured areas.
- Use a privacy screen.
- Lock your workstation.
- Keep access badges and keys secure at all times.
- Secure Documents.
- Appropriately discard or shred sensitive documents.

Confidential info (Slide Layer)

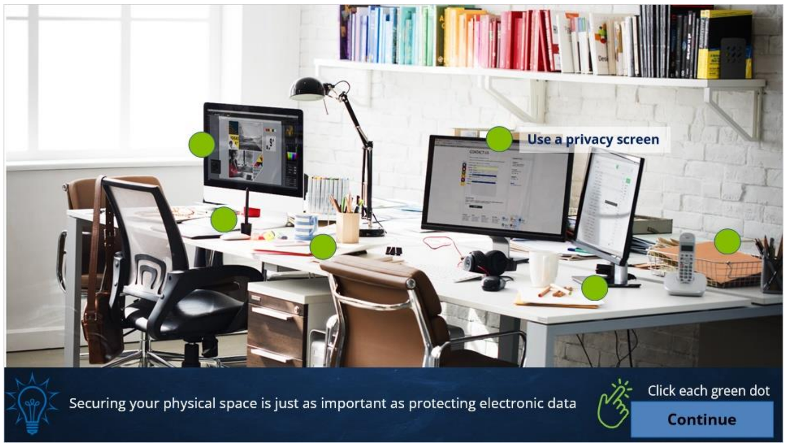


Don't leave confidential and/or sensitive information in unsecured areas

Securing your physical space is just as important as protecting electronic data

Click each green dot

Privacy Screen (Slide Layer)

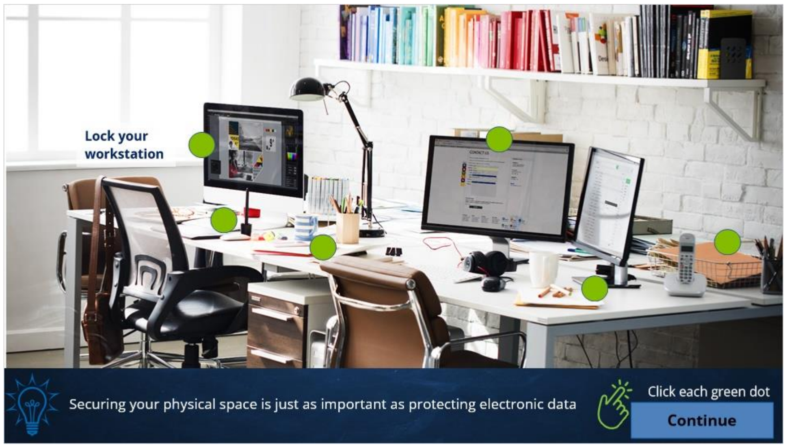


Use a privacy screen

Securing your physical space is just as important as protecting electronic data

Click each green dot

Lock Workstation (Slide Layer)

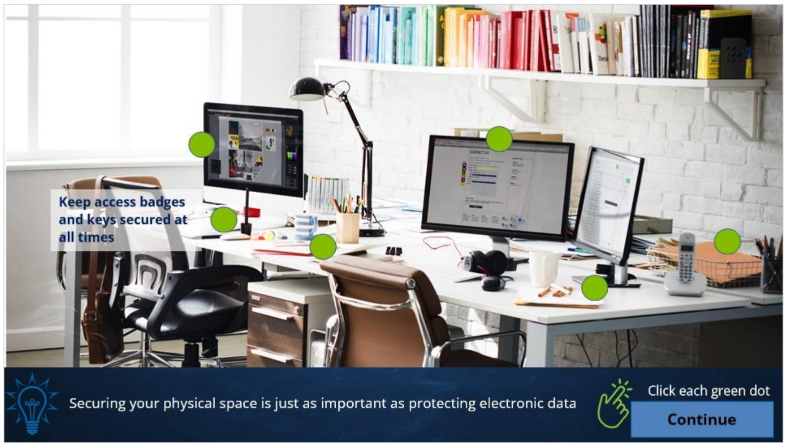


Lock your workstation

Securing your physical space is just as important as protecting electronic data

Click each green dot

Access Badge (Slide Layer)

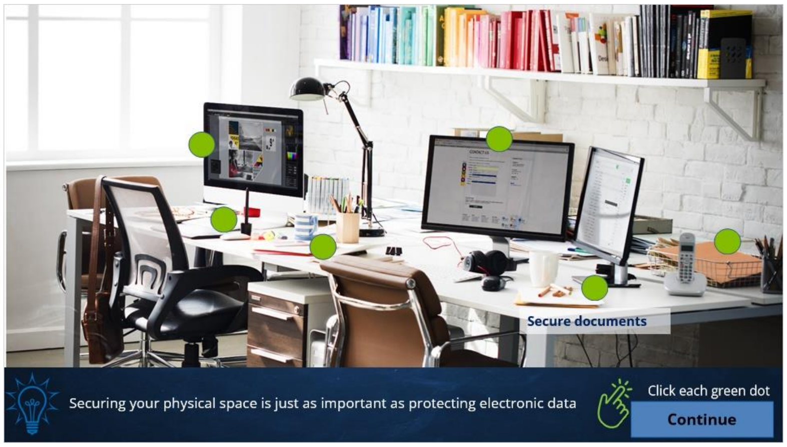


Keep access badges and keys secured at all times

Securing your physical space is just as important as protecting electronic data

Click each green dot

Secure Docs (Slide Layer)

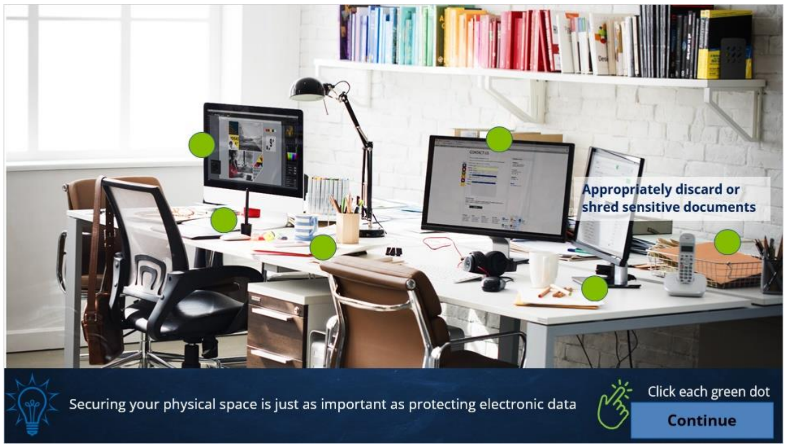


Secure documents

Securing your physical space is just as important as protecting electronic data

Click each green dot

Shred or Discard (Slide Layer)

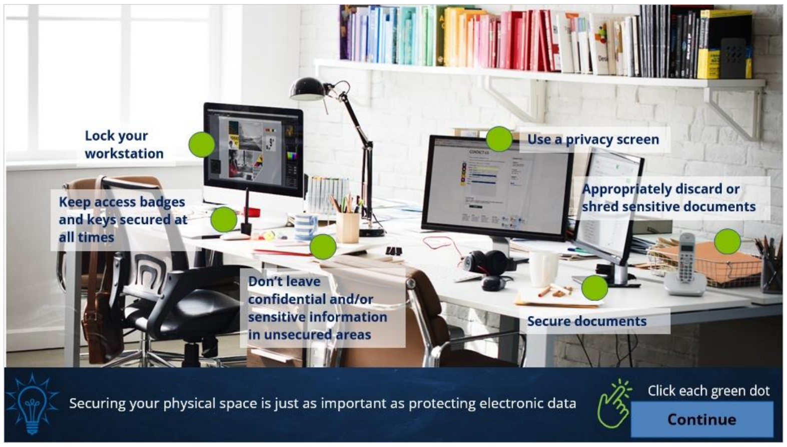


Appropriately discard or shred sensitive documents

Securing your physical space is just as important as protecting electronic data

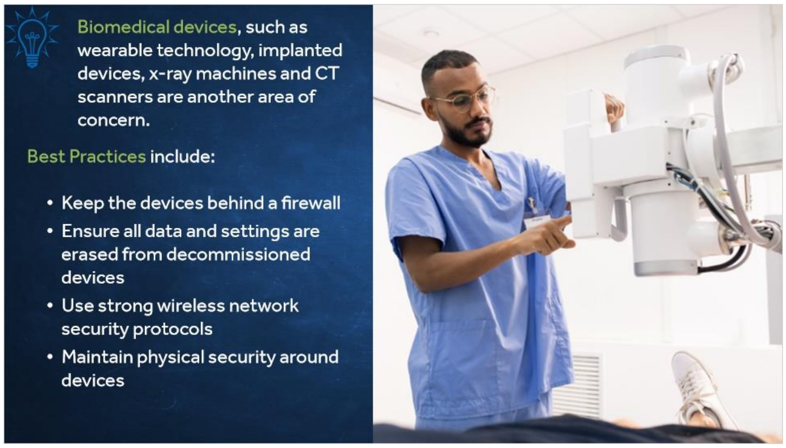
Click each green dot

Final (Slide Layer)


Lock your workstation
Use a privacy screen
Keep access badges and keys secured at all times
Appropriately discard or shred sensitive documents
Don't leave confidential and/or sensitive information in unsecured areas
Secure documents
Click each green dot
Continue

Securing your physical space is just as important as protecting electronic data

1.20 Biomedical Devices



Biomedical devices, such as wearable technology, implanted devices, x-ray machines and CT scanners are another area of concern.

Best Practices include:

- Keep the devices behind a firewall
- Ensure all data and settings are erased from decommissioned devices
- Use strong wireless network security protocols
- Maintain physical security around devices

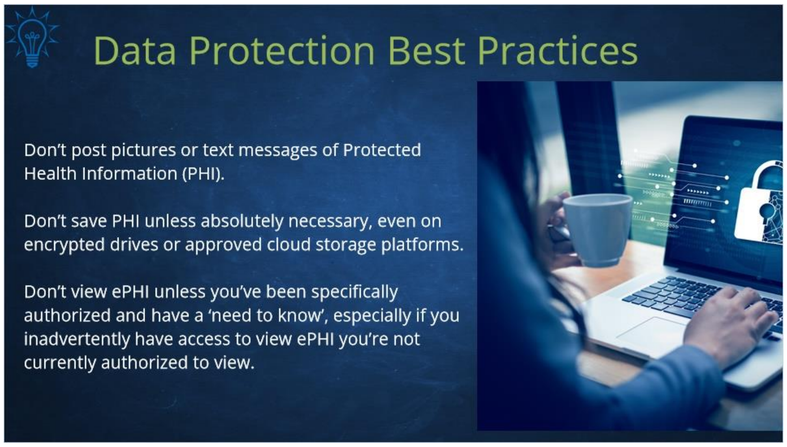
Notes:

Biomedical devices, such as wearable technology, implanted devices, x-ray machines, and CT scanners, are another area of concern.

Best Practices include:

- Keep the devices behind a firewall
- Ensure all data and settings are erased from decommissioned devices
- Use strong wireless network security protocols
- Maintain physical security around devices

1.21 Data Protection Best Practices



Data Protection Best Practices

Don’t post pictures or text messages of Protected Health Information (PHI).

Don’t save PHI unless absolutely necessary, even on encrypted drives or approved cloud storage platforms.

Don’t view ePHI unless you’ve been specifically authorized and have a ‘need to know’, especially if you inadvertently have access to view ePHI you’re not currently authorized to view.

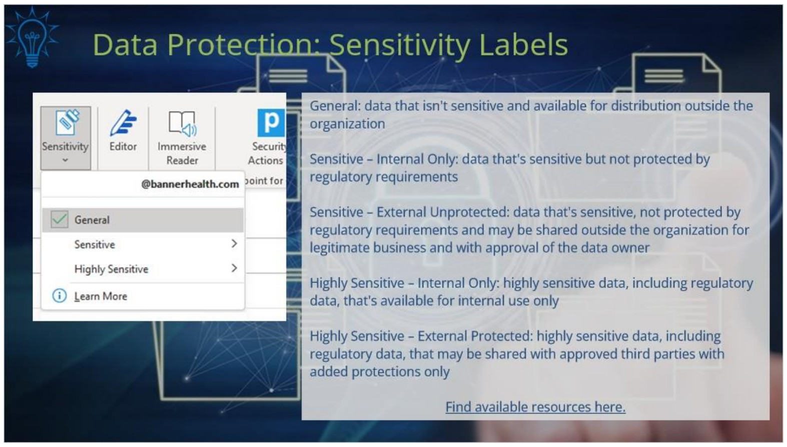
Notes:

Don’t post pictures or text messages of Protected Health Information (PHI).

Don’t save PHI unless absolutely necessary, even on encrypted drives or approved cloud storage platforms.

Don’t view ePHI unless you’ve been specifically authorized and have a ‘need to know’, especially if you inadvertently have access to view ePHI you’re not currently authorized to view.

1.22 Data Protection Best Practices



Data Protection: Sensitivity Labels

General: data that isn't sensitive and available for distribution outside the organization

Sensitive – Internal Only: data that's sensitive but not protected by regulatory requirements

Sensitive – External Unprotected: data that's sensitive, not protected by regulatory requirements and may be shared outside the organization for legitimate business and with approval of the data owner

Highly Sensitive – Internal Only: highly sensitive data, including regulatory data, that's available for internal use only

Highly Sensitive – External Protected: highly sensitive data, including regulatory data, that may be shared with approved third parties with added protections only

Find available resources here.

Notes:

Using sensitivity labels also helps protect sensitive information.

General: data that isn't sensitive and available for distribution outside the organization

Sensitive – Internal Only: data that's sensitive but not protected by regulatory requirements

Sensitive – External Unprotected: data that's sensitive, not protected by regulatory requirements and may be shared outside the organization for legitimate business and with approval of the data owner

Highly Sensitive – Internal Only: highly sensitive data, including regulatory data, that's available for internal use only

Highly Sensitive – External Protected: highly sensitive data, including regulatory data, that may be shared with approved third parties with added protections only

1.23 Payment Card Industry 1

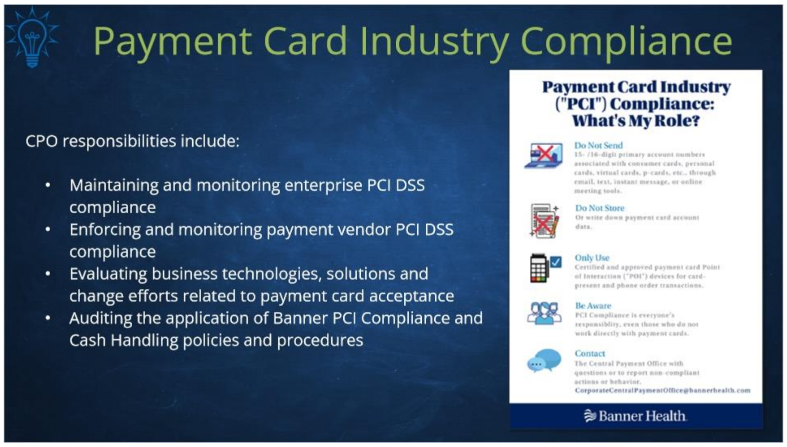
Payment Card Industry Compliance

Banner formed the Central Payment Office (CPO) within the Treasury department to ensure systemwide compliance with the Payment Card Industry Data Security Standard (PCI DSS) requirements.

Notes:

Banner formed the Central Payment Office ("CPO") within the Treasury department to ensure enterprise-wide compliance with the Payment Card Industry Data Security Standard (“PCI DSS”) requirements.

1.24 Payment Card Industry 2



Payment Card Industry Compliance

CPO responsibilities include:

- Maintaining and monitoring enterprise PCI DSS compliance
- Enforcing and monitoring payment vendor PCI DSS compliance
- Evaluating business technologies, solutions and change efforts related to payment card acceptance
- Auditing the application of Banner PCI Compliance and Cash Handling policies and procedures

Payment Card Industry ("PCI") Compliance: What's My Role?

Do Not Send
15- /16-digit primary account numbers associated with consumer cards, personal cards, virtual cards, p-cards, etc., through email, text, instant message, or online meeting tools.

Do Not Store
Or write down payment card account data.

Only Use
Certified and approved payment card Point of Interaction ("POI") devices for card-present and phone order transactions.

Be Aware
PCI Compliance is everyone's responsiblity, even those who do not work directly with payment cards.

Contact
The Central Payment Office with questions or to report non-compliant actions or behavior.
CorporateCentralPaymentOffice@bannerhealth.com

Banner Health

Notes:

CPO responsibilities include:

- Maintaining and monitoring enterprise PCI DSS compliance;
- Enforcing and monitoring payment vendor PCI DSS compliance;
- Evaluating business technologies, solutions, and change efforts related to payment card acceptance; and
- Auditing the application of Banner PCI Compliance and Cash Handling policies and procedures.

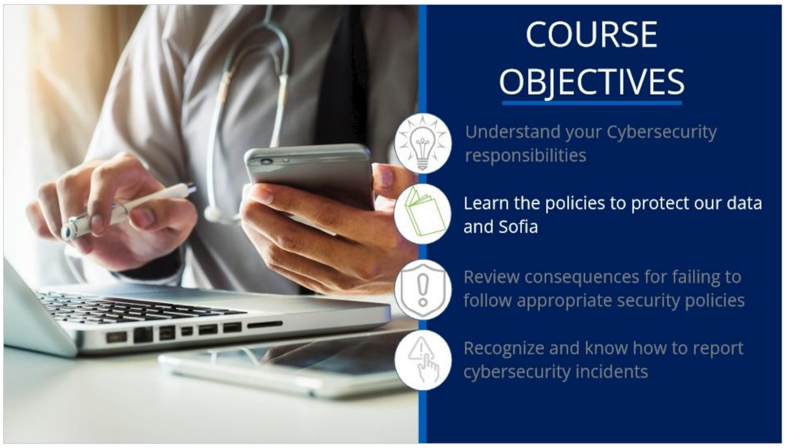
As part of your role in helping Banner maintain PCI compliance,

- Do not send 15- /16-digit primary account numbers associated with consumer cards, personal cards, virtual cards, p-cards, etc., through email, text, instant message, or online meeting tools;
- Do not store or write down payment card account data; and
- Only use certified and approved payment card Point of Interaction

("POI") devices for card-present and phone order transactions.

PCI compliance is the responsibility of all Banner employees, even those who do not directly handle payment card data. If you notice any suspicious or non-compliant behavior related to payment card processes or solutions (e.g., evidence of tampering with the payment card POI devices, attempts to record and steal payment card data, unfamiliar payment portals or technologies used for collecting payment cards, etc.), please contact the CPO.

1.25 Objective 2



COURSE OBJECTIVES

- Understand your Cybersecurity responsibilities
- Learn the policies to protect our data and Sofia
- Review consequences for failing to follow appropriate security policies
- Recognize and know how to report cybersecurity incidents

Notes:

Now that you have a better understanding of your responsibilities when it comes to cybersecurity, let's look at the second objective.

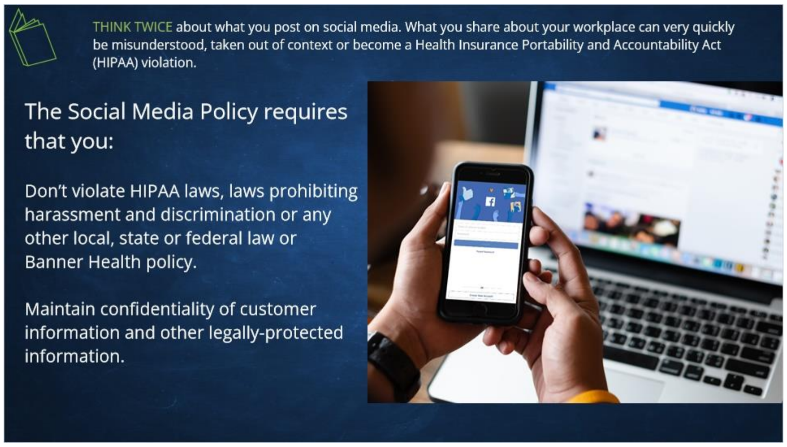
1.26 Policies

Learn Policies to Protect our Data and Sofia

Notes:

Here we'll highlight some important policies that help protect our data and Sofia.

1.27 Social Media Policy 1



THINK TWICE about what you post on social media. What you share about your workplace can very quickly be misunderstood, taken out of context or become a Health Insurance Portability and Accountability Act (HIPAA) violation.

The Social Media Policy requires that you:

Don't violate HIPAA laws, laws prohibiting harassment and discrimination or any other local, state or federal law or Banner Health policy.

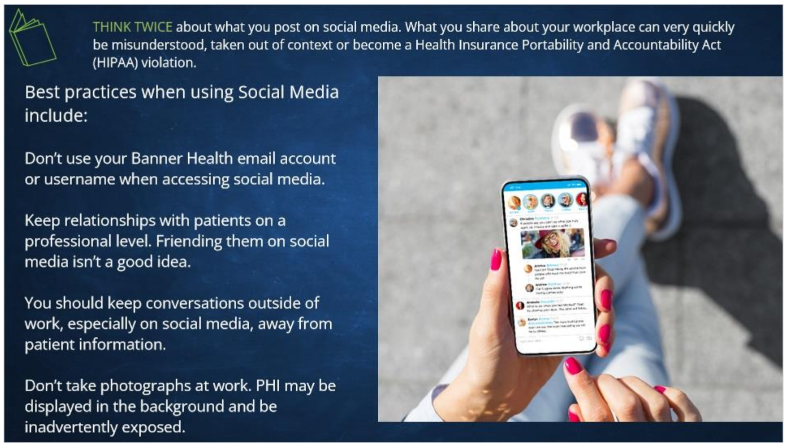
Maintain confidentiality of customer information and other legally-protected information.

Notes:

Most of us use social media platforms like Facebook, Twitter, Instagram, and others, but you need to think twice about what you post. What you share about your workplace can quickly be misunderstood, taken out of context, or become a HIPAA violation.

The Social Media Policy requires that you do not violate any laws or Banner Health policy and that you maintain confidentiality of patient information and other legally-protected information.

1.28 Social Media Policy 2



THINK TWICE about what you post on social media. What you share about your workplace can very quickly be misunderstood, taken out of context or become a Health Insurance Portability and Accountability Act (HIPAA) violation.

Best practices when using Social Media include:

Don't use your Banner Health email account or username when accessing social media.

Keep relationships with patients on a professional level. Friending them on social media isn't a good idea.

You should keep conversations outside of work, especially on social media, away from patient information.

Don't take photographs at work. PHI may be displayed in the background and be inadvertently exposed.

Notes:

And remember, don't use your Banner Health email account or username when accessing social media.

Keep relationships with patients on a professional level. Friending them on social media is not a good idea.

You should keep conversations outside of work, especially on social media, away from patient information.

Do *not* take photographs at work as PHI may be displayed in the background and could be inadvertently exposed.

1.29 International Travel 1

International Travel and Remote Working Requirements

Don’t take your Banner-issued laptop or other devices out of the United States for vacations and/or to work remotely; a temporary Banner-issued loaner device is available if the request to work internationally is approved.

You should submit your request at least three weeks before travel is scheduled.

Remember, team members aren’t authorized to use their personally-owned laptop for Banner business or connect to the Banner network or systems when working internationally.

Notes:

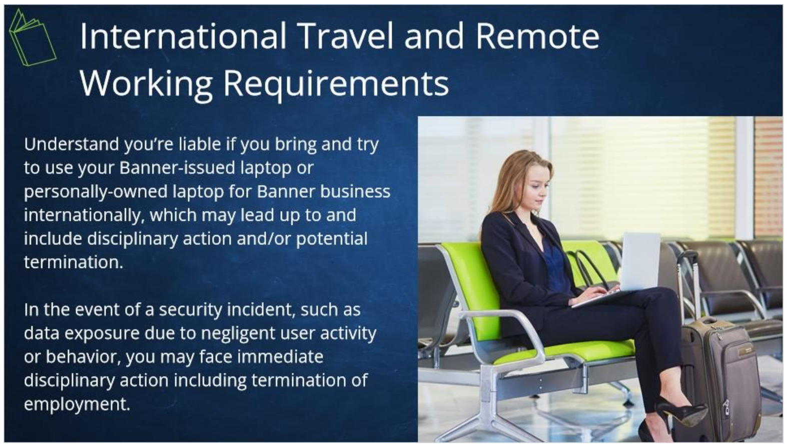
If you have a need to work internationally, please contact IT Cybersecurity prior to departing to ensure you have the appropriate controls in place to keep your information and Banner’s safe from inadvertent disclosure.

Don’t take your Banner-issued laptop or other devices out of the United States for vacations and/or to work remotely; a temporary Banner-issued loaner device is available if the request to work internationally is approved.

You should submit your request at least three weeks before travel is scheduled.

Remember, team members aren’t authorized to use their personally-owned laptop for Banner business or connect to the Banner network or systems when working internationally.

1.30 International Travel 2



International Travel and Remote Working Requirements

Understand you're liable if you bring and try to use your Banner-issued laptop or personally-owned laptop for Banner business internationally, which may lead up to and include disciplinary action and/or potential termination.

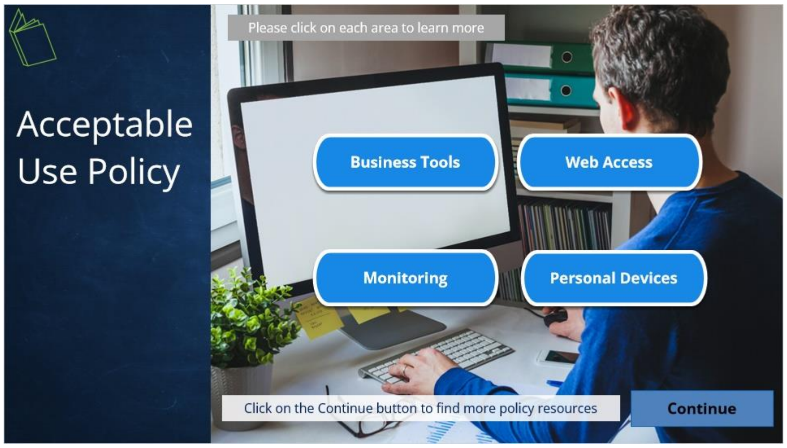
In the event of a security incident, such as data exposure due to negligent user activity or behavior, you may face immediate disciplinary action including termination of employment.

Notes:

Understand that you're liable if you bring and try to use your Banner issued laptop or personally owned laptop for Banner business internationally, which may lead up to and include disciplinary action and/or potential termination.

In the event of a security incident such as data exposure due to negligent user activity or behavior, you may face immediate disciplinary action including termination of employment.

1.31 Acceptable Use Policy



Acceptable Use Policy

Please click on each area to learn more

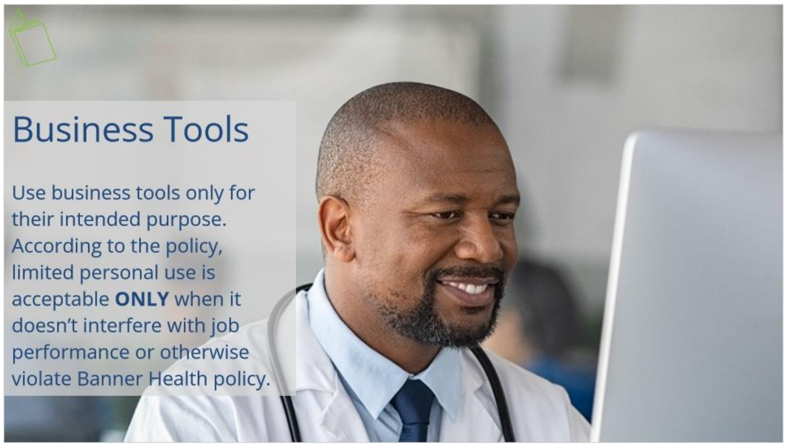
Click on the Continue button to find more policy resources

Notes:

The Acceptable Use policy is like the umbrella policy for all of Information

Technology. Most questions team members have concerning device usage can be found in this policy. Highlighted on the screen are four areas of the Acceptable Use policy. Please click on each button to learn more.

1.32 Business Tools



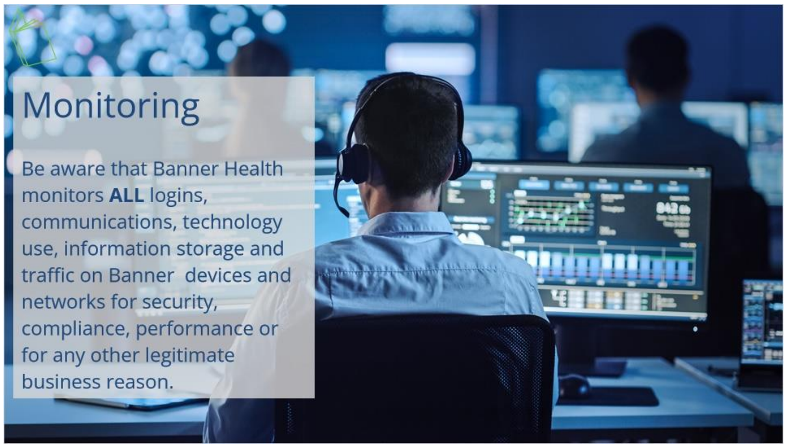
Business Tools

Use business tools only for their intended purpose. According to the policy, limited personal use is acceptable **ONLY** when it doesn't interfere with job performance or otherwise violate Banner Health policy.

Notes:

Use business tools only for their intended purpose. According to the policy, limited personal use is acceptable **ONLY** when it does not interfere with job performance or otherwise violate Banner Health policy.

1.33 Monitoring



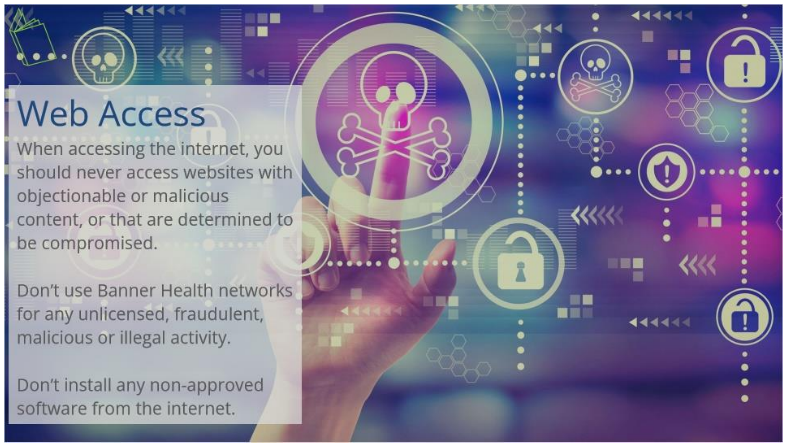
Monitoring

Be aware that Banner Health monitors **ALL** logins, communications, technology use, information storage and traffic on Banner devices and networks for security, compliance, performance or for any other legitimate business reason.

Notes:

Be aware that Banner Health monitors **ALL** communication, technology use, information storage, and traffic on Banner Health devices and networks for security, compliance, performance, or any other legitimate business reason.

1.34 Web Access



Web Access

When accessing the internet, you should never access websites with objectionable or malicious content, or that are determined to be compromised.

Don't use Banner Health networks for any unlicensed, fraudulent, malicious or illegal activity.

Don't install any non-approved software from the internet.

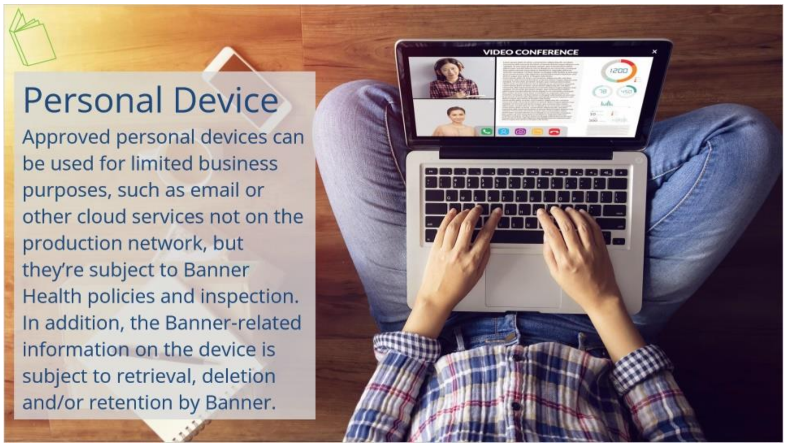
Notes:

When accessing the internet, you should never access websites with objectionable or malicious content, or that are determined to be compromised.

Don't use Banner Health networks for any unlicensed, fraudulent, malicious or illegal activity.

Don't install any non-approved software from the internet.

1.35 Personal Device



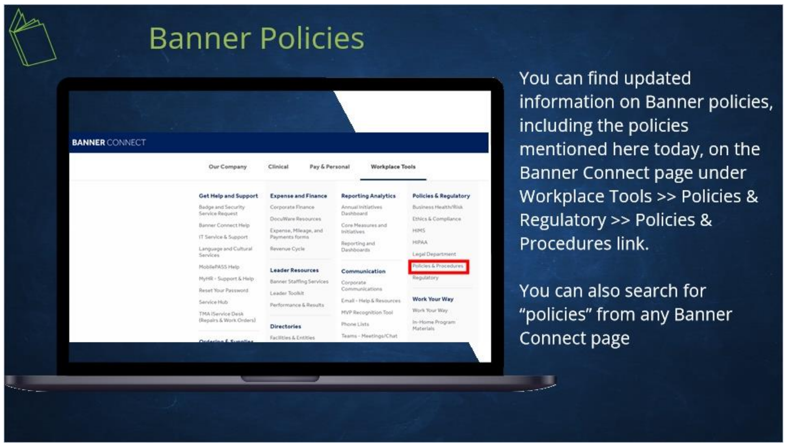
Personal Device

Approved personal devices can be used for limited business purposes, such as email or other cloud services not on the production network, but they're subject to Banner Health policies and inspection. In addition, the Banner-related information on the device is subject to retrieval, deletion and/or retention by Banner.

Notes:

Approved personal devices can be used for limited business purposes, such as email or other cloud services not on the production network, but they're subject to Banner Health policies and inspection. In addition, the Banner-related information on the device is subject to retrieval, deletion and/or retention by Banner.

1.36 Policy Resources



Banner Policies

You can find updated information on Banner policies, including the policies mentioned here today, on the Banner Connect page under Workplace Tools >> Policies & Regulatory >> Policies & Procedures link.

You can also search for "policies" from any Banner Connect page

Notes:

You can find updated information on Banner policies, including the policies mentioned here today, on the Banner Connect page under Workplace Tools >>

Policies & Regulatory >> Policies & Procedures link.

You can also search for “policies” from any Banner Connect page

1.37 Objective 3

COURSE OBJECTIVES

Understand your Cybersecurity responsibilities

Learn the policies to protect our data and Sofia

Review consequences for failing to follow appropriate security policies

Recognize and know how to report cybersecurity incidents

Notes:

We now know our cybersecurity responsibilities and learned about some of the policies to protect Sofia and our data. Let’s now look at the third objective.

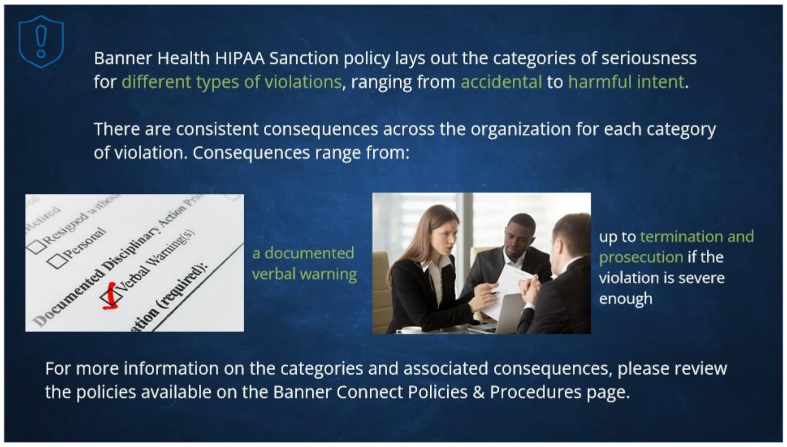
1.38 Consequences 1

Review Consequences for Failing to Follow Appropriate Security Policies

Notes:

Actions have consequences--whether they’re positive or negative. In the event of failing to adhere to Banner policies, there are consequences that could affect your term of employment.

1.39 Consequences 2



Banner Health HIPAA Sanction policy lays out the categories of seriousness for different types of violations, ranging from accidental to harmful intent.

There are consistent consequences across the organization for each category of violation. Consequences range from:

a documented verbal warning

up to termination and prosecution if the violation is severe enough

For more information on the categories and associated consequences, please review the policies available on the Banner Connect Policies & Procedures page.

Notes:

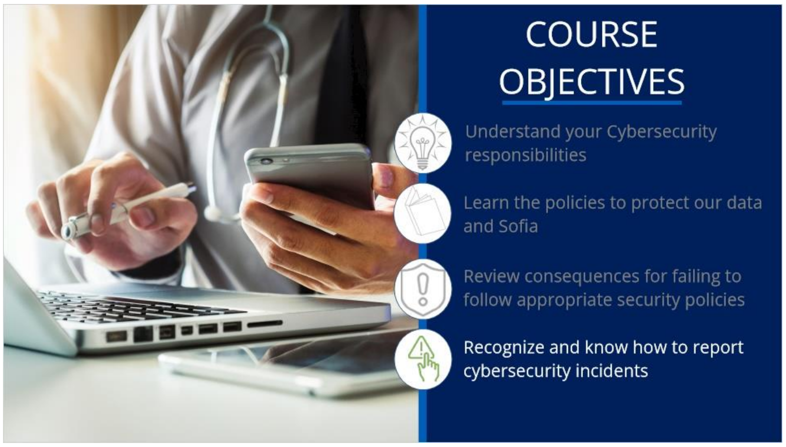
Banner recognizes that mistakes can happen, so not all consequences are the same. Consequences depend on the severity of the violation. Banner Health policy outlines the categories of seriousness for different types of violations, ranging from accidental to harmful intent.

There are consistent consequences across the organization for each violation category. Consequences range from a documented verbal warning, up to termination and prosecution if the violation is severe enough.

For more information on the categories and associated consequences, please review the policies available on the homepage.

If you see something, say something. Part of doing the right thing in accordance with the policy is fulfilling your obligation to report any potential violation you witness.

1.40 Objective 4



COURSE OBJECTIVES

- Understand your Cybersecurity responsibilities
- Learn the policies to protect our data and Sofia
- Review consequences for failing to follow appropriate security policies
- Recognize and know how to report cybersecurity incidents

Notes:

And, finally, let’s look at our last objective.

1.41 Report Cybersecurity Incidents

Recognize and Know How to Report Cybersecurity Incidents

Notes:

Let’s wrap it up by going over some common cybersecurity incidents and what you should do in the event you come across one.

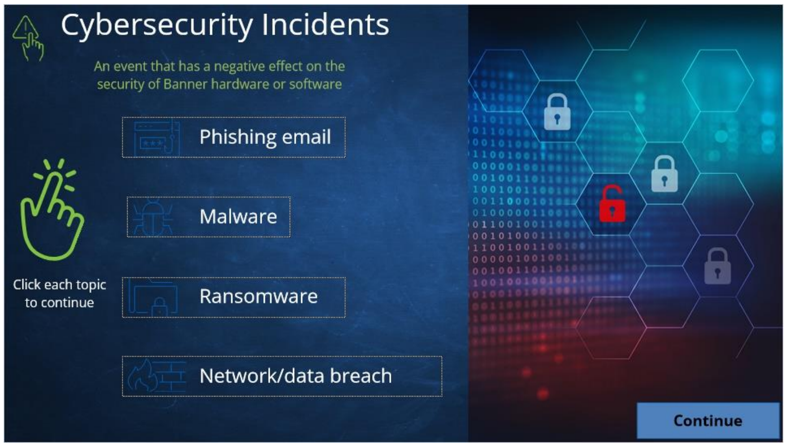
1.42 See something, say something

If you see something, say something.

Notes:

As we just mentioned, part of doing the right thing, in accordance with policy as a Banner team member, is to report any potential violation you witness, which includes cybersecurity incidents such as phishing emails, a suspicious individual in a secured area or even a lost or stolen device. We can't be everywhere, so we need your help to keep Banner, Sofia and you safe and secure. Remember, if you see something, say something.

1.43 Cybersecurity Incident Events



Cybersecurity Incidents

An event that has a negative effect on the security of Banner hardware or software

Click each topic to continue

Notes:

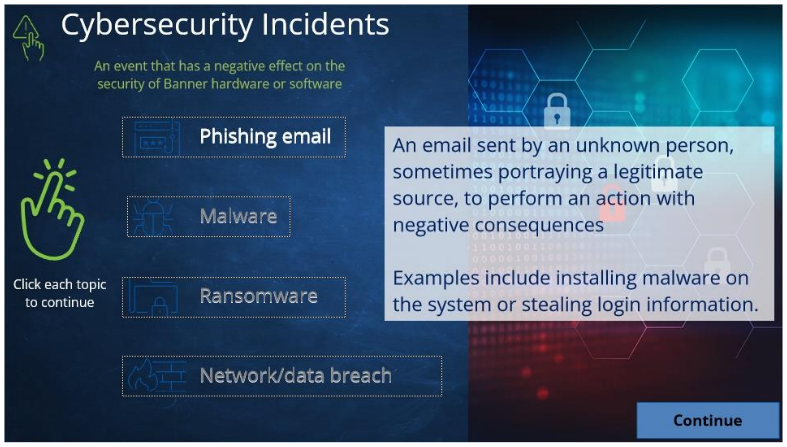
A cybersecurity Incident is an event that has a negative effect on the security of

Banner Health hardware or software.

Click each icon to learn what these terms mean at Banner Health.

- **Phishing email**: An email sent by an unknown person, sometimes portraying a legitimate source, to perform an action with negative consequences. Examples include installing malware on the system or stealing login information
- **Malware:** Software that can perform actions on a system or network without permission. Examples include viruses, worms, ransomware, spyware and Trojan horses
- **Ransomware:** Malicious software that infects your computer and displays messages demanding a fee to be paid in order for your system to work again. Has the ability to lock a computer screen or encrypt important, predetermined files with a password.
- **Network/Data Breach:** An incident where an individual has purposely or indirectly leaked or stolen confidential information.This can involve Protected Health Information (PHI), Personally Identifiable Information (PII) or Payment Card Information (PCI

Phishing Email (Slide Layer)



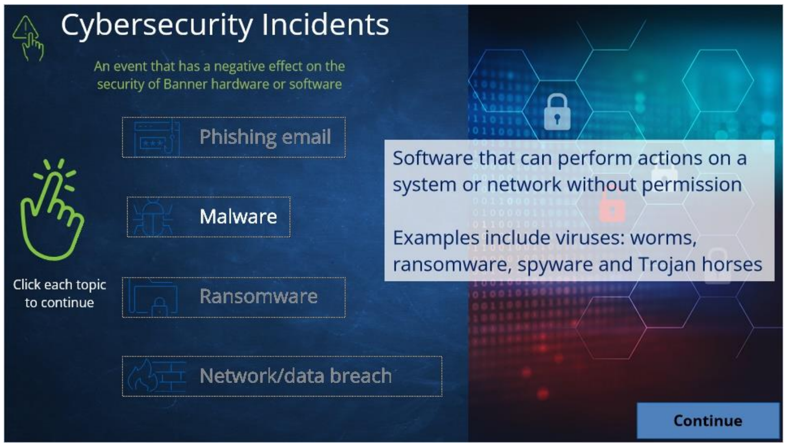
Cybersecurity Incidents

An event that has a negative effect on the security of Banner hardware or software

An email sent by an unknown person, sometimes portraying a legitimate source, to perform an action with negative consequences

Examples include installing malware on the system or stealing login information.

Malware (Slide Layer)



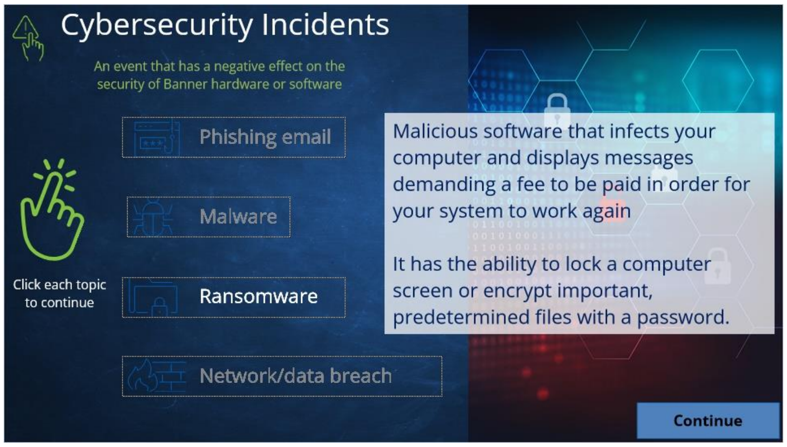
Cybersecurity Incidents

An event that has a negative effect on the security of Banner hardware or software

Software that can perform actions on a system or network without permission

Examples include viruses: worms, ransomware, spyware and Trojan horses

Ransomware (Slide Layer)



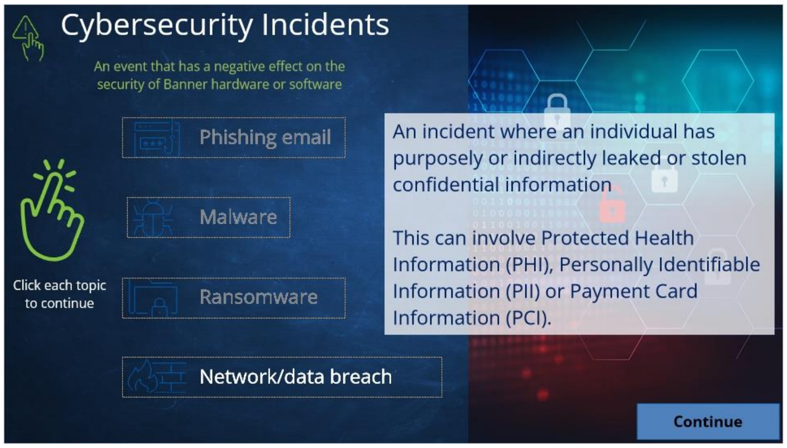
Cybersecurity Incidents

An event that has a negative effect on the security of Banner hardware or software

Malicious software that infects your computer and displays messages demanding a fee to be paid in order for your system to work again

It has the ability to lock a computer screen or encrypt important, predetermined files with a password.

Network/Data Breach (Slide Layer)



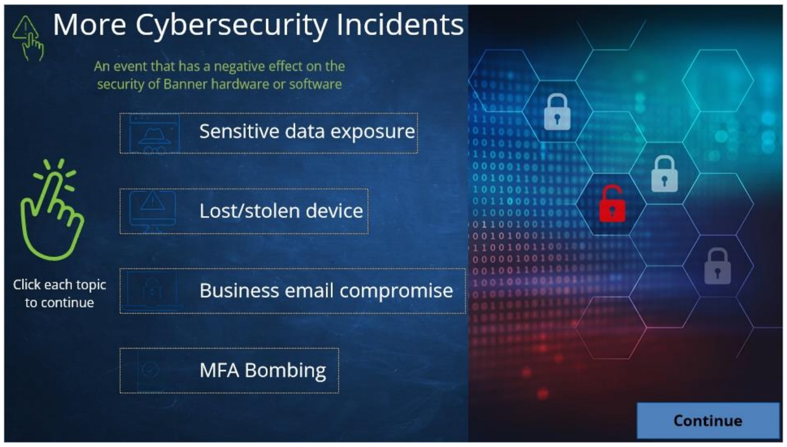
Cybersecurity Incidents

An event that has a negative effect on the security of Banner hardware or software

An incident where an individual has purposely or indirectly leaked or stolen confidential information

This can involve Protected Health Information (PHI), Personally Identifiable Information (PII) or Payment Card Information (PCI).

1.44 Cybersecurity Incident Events



More Cybersecurity Incidents

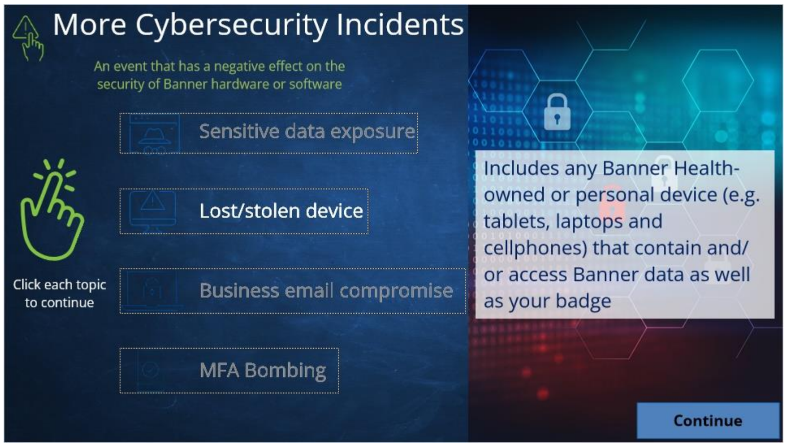
An event that has a negative effect on the security of Banner hardware or software

Click each topic to continue

Notes:

- Sensitive data Exposure: Proper security controls are not in place, allowing easy access to information that should *not* be shared. An example is when there is no password used to access an application
- Lost/stolen device: Includes any Banner Health owned or personal device (e.g. tablets, laptops and cellphones) that contain and/or access Banner Health data
- Business Email Compromise: Attackers compromise or spoof trusted email addresses to trick users into performing fraudulent wire transfers or other financial scams.
- MFA Bombing: Attackers send multiple MFA prompts to approve signing in. Only approve MFA requests that you facilitated.

Lost/stolen device (Slide Layer)

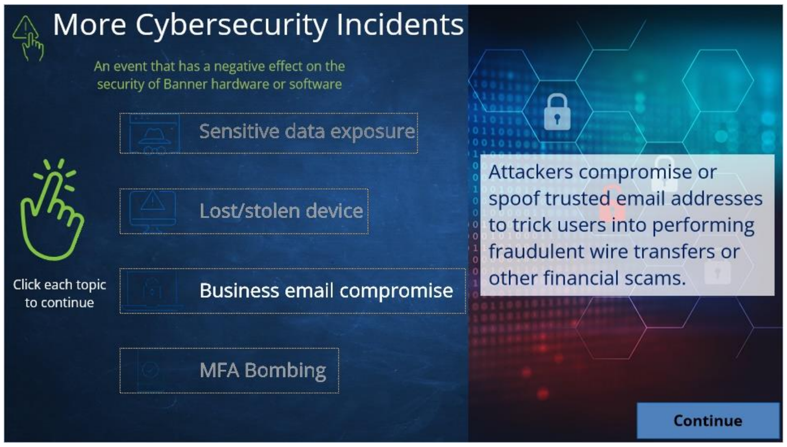


More Cybersecurity Incidents

An event that has a negative effect on the security of Banner hardware or software

Includes any Banner Health-owned or personal device (e.g. tablets, laptops and cellphones) that contain and/or access Banner data as well as your badge

Business Email Compromise (Slide Layer)

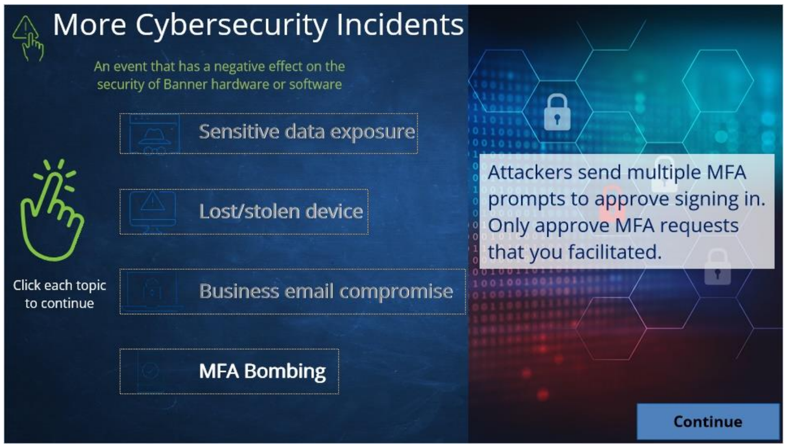


More Cybersecurity Incidents

An event that has a negative effect on the security of Banner hardware or software

Attackers compromise or spoof trusted email addresses to trick users into performing fraudulent wire transfers or other financial scams.

MFA Bombing (Slide Layer)

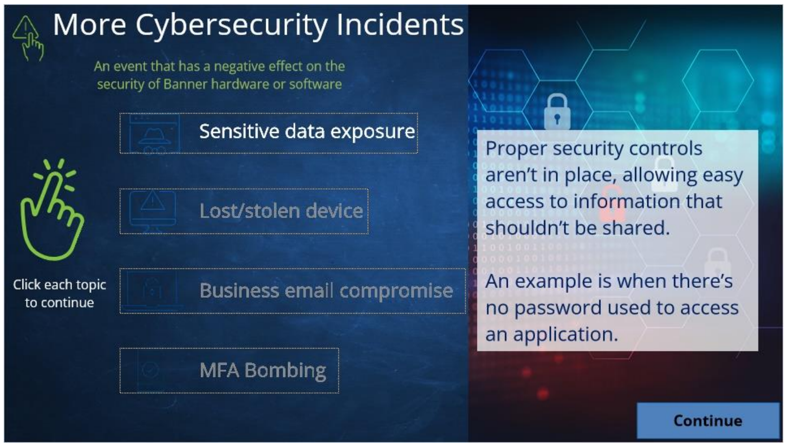


More Cybersecurity Incidents

An event that has a negative effect on the security of Banner hardware or software

Attackers send multiple MFA prompts to approve signing in. Only approve MFA requests that you facilitated.

Sensitive Data Exposure (Slide Layer)



More Cybersecurity Incidents

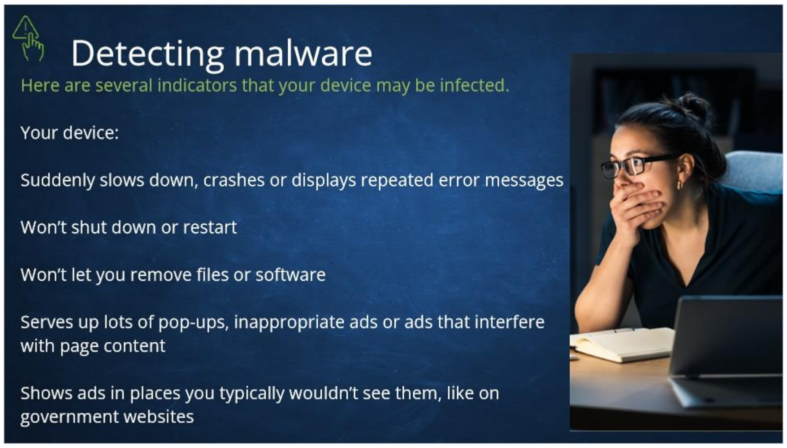
An event that has a negative effect on the security of Banner hardware or software

Click each topic to continue

Proper security controls aren't in place, allowing easy access to information that shouldn't be shared.

An example is when there's no password used to access an application.

1.45 Detecting Malware



Detecting malware

Here are several indicators that your device may be infected.

Your device:

Suddenly slows down, crashes or displays repeated error messages

Won't shut down or restart

Won't let you remove files or software

Serves up lots of pop-ups, inappropriate ads or ads that interfere with page content

Shows ads in places you typically wouldn't see them, like on government websites

Notes:

Here are several indicators that your device may be infected.
Your device:

Suddenly slows down, crashes or displays repeated error messages

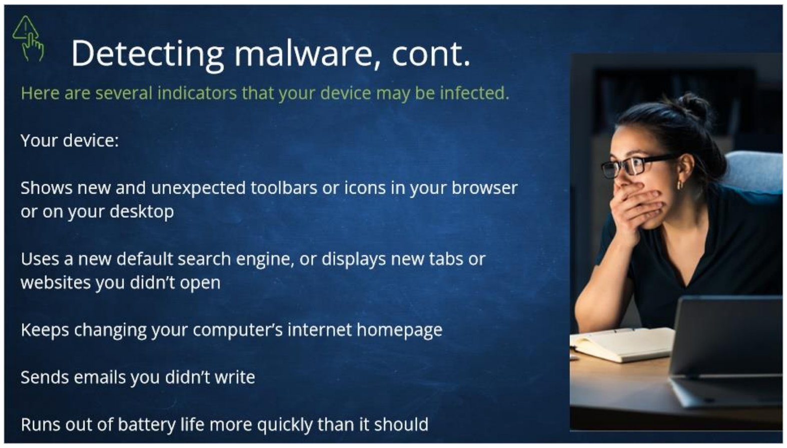
Won't shut down or restart

Won't let you remove files or software

Serves up lots of pop-ups, inappropriate ads or ads that interfere with page content

Shows ads in places you typically wouldn't see them, like on government websites

1.46 Detecting Malware 2



Detecting malware, cont.

Here are several indicators that your device may be infected.

Your device:

Shows new and unexpected toolbars or icons in your browser or on your desktop

Uses a new default search engine, or displays new tabs or websites you didn't open

Keeps changing your computer's internet homepage

Sends emails you didn't write

Runs out of battery life more quickly than it should

Notes:

Shows new and unexpected toolbars or icons in your browser or on your desktop,

Uses a new default search engine, or displays new tabs or websites you didn't open,

Keeps changing your computer's internet homepage,

Sends emails you didn't write,

Runs out of battery life more quickly than it should

1.47 Insider Threats

Insider Threats

Insiders become a risk when they willingly, knowingly or inadvertently use their level of access to harm the organization or other employees. One of the most common insider risk scenarios is when employees leave an organization and attempt to take files and data with them to their future employer.

This data may include trade secrets, pricing data or sales and opportunity information that could negatively impact the organization it belongs to.

If you see something, say something.

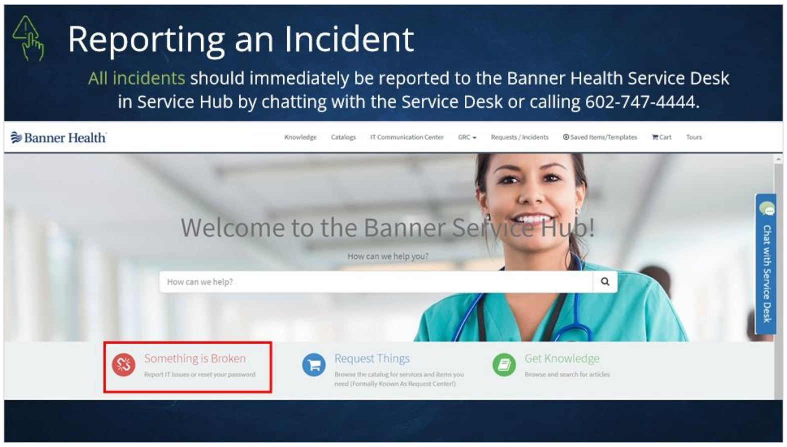
Notes:

Insiders become a risk when they willingly, knowingly or inadvertently use their level of access to harm the organization or other employees. One of the most common insider risk scenarios is when employees leave an organization and attempt to take files and data with them to their future employer.

This data may include trade secrets, pricing data or sales and opportunity information that could negatively impact the organization it belongs to.

If you see something, say something.

1.48 Report an Incident



Reporting an Incident

All incidents should immediately be reported to the Banner Health Service Desk in Service Hub by chatting with the Service Desk or calling 602-747-4444.

Notes:

All potential Security incidents should be reported to the Banner Health Service Desk in Service Hub, by chatting with the Service Desk or by calling **602-747-4444.**

1.49 Additional Resources

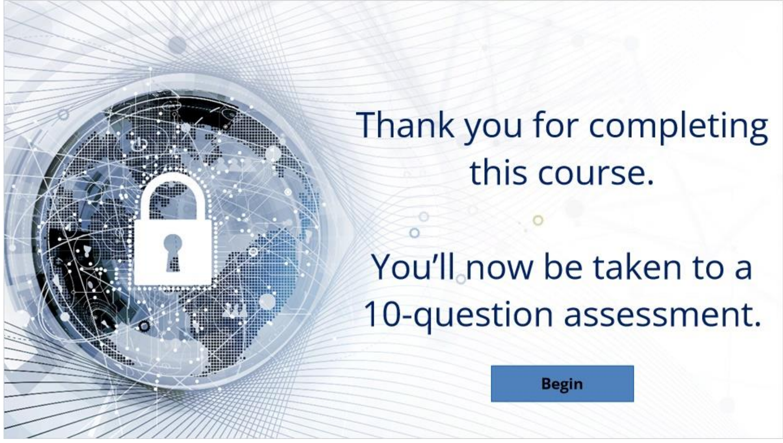
ADDITIONAL RESOURCES

Click the icon to access our IT Cybersecurity and Privacy Resource Library bookshelf.

Notes:

If you'd like to learn more about cybersecurity or privacy topics, before exiting this course, please click the icon to access our IT Cybersecurity and Privacy Resource Library.

1.50 Thank You



Thank you for completing this course.

You'll now be taken to a 10-question assessment.

Notes:

This concludes this portion of the course. We hope you learned about Cybersecurity and your important role in helping protect our patients' data.

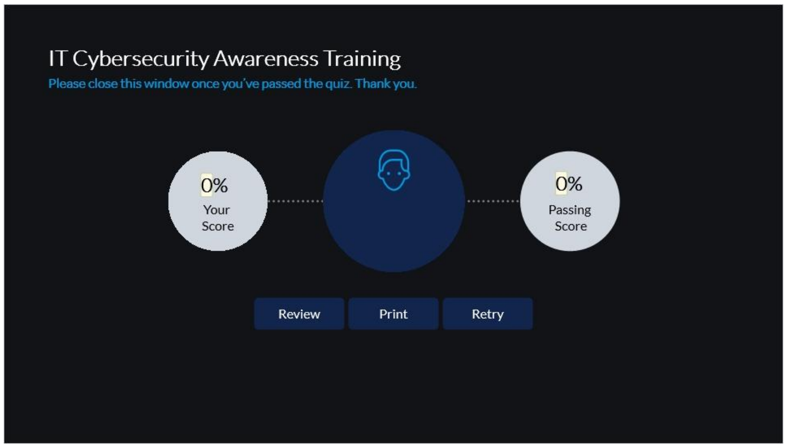
You'll now be taken to a 10-question assessment. You must score an 80% or better to receive credit for this course. Thank you and have a great day.

1.51 Draw from Cybersecurity

Draw 10 questions randomly from Cybersecurity

1.52 IT Cybersecurity Awareness Training

(Results Slide, 0 points, 1 attempt permitted)



IT Cybersecurity Awareness Training

Please close this window once you've passed the quiz. Thank you.

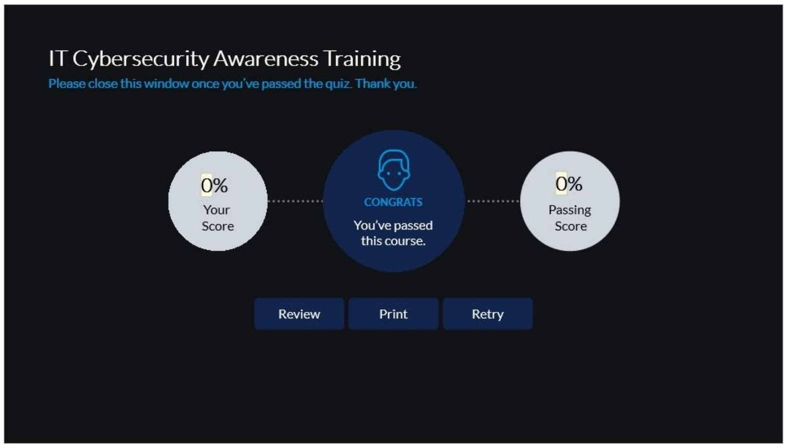
Results for
1.51 Draw from Cybersecurity

Result slide properties

Passing Score	80%

Notes:

Success (Slide Layer)



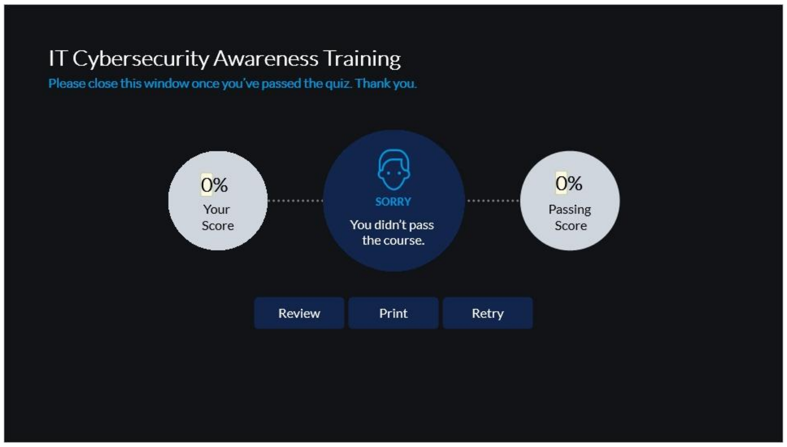
IT Cybersecurity Awareness Training

Please close this window once you've passed the quiz. Thank you.

CONGRATS

You've passed this course.

Failure (Slide Layer)



IT Cybersecurity Awareness Training

Please close this window once you've passed the quiz. Thank you.

0% Your Score

SORRY

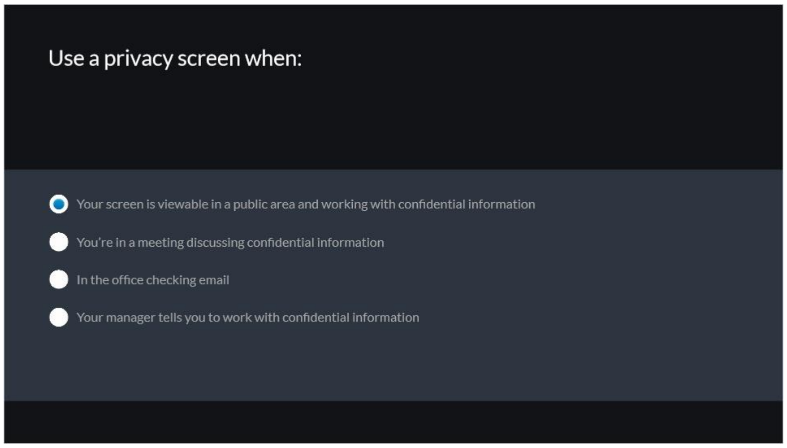
You didn't pass the course.

0% Passing Score

2. Cybersecurity

Q2.1 MULTIPLE CHOICE QUESTION

(Multiple Choice, 10 points, 1 attempt permitted)



Use a privacy screen when:

● Your screen is viewable in a public area and working with confidential information

○ You're in a meeting discussing confidential information

○ In the office checking email

○ Your manager tells you to work with confidential information

Correct	Choice
X	Your screen is viewable in a public area and working with confidential information
	You're in a meeting discussing confidential information
	In the office checking email

Your manager tells you to work with confidential information

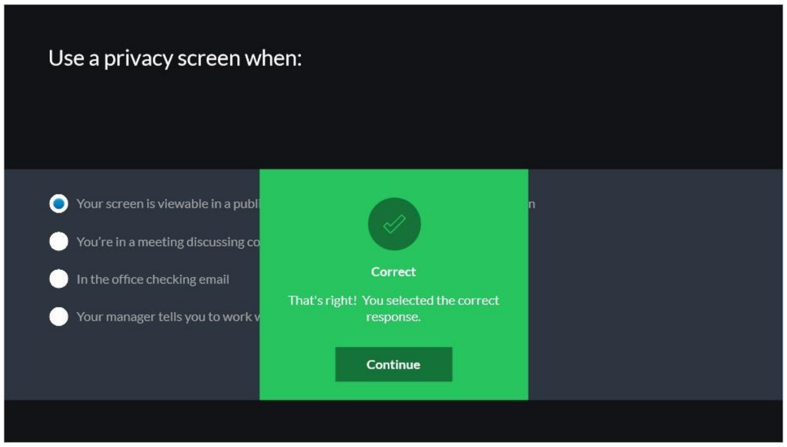
Feedback when correct:

That's right! You selected the correct response.

Feedback when incorrect:

You did not select the correct response.

Correct (Slide Layer)



Use a privacy screen when:

● Your screen is viewable in a publ n

○ You're in a meeting discussing co

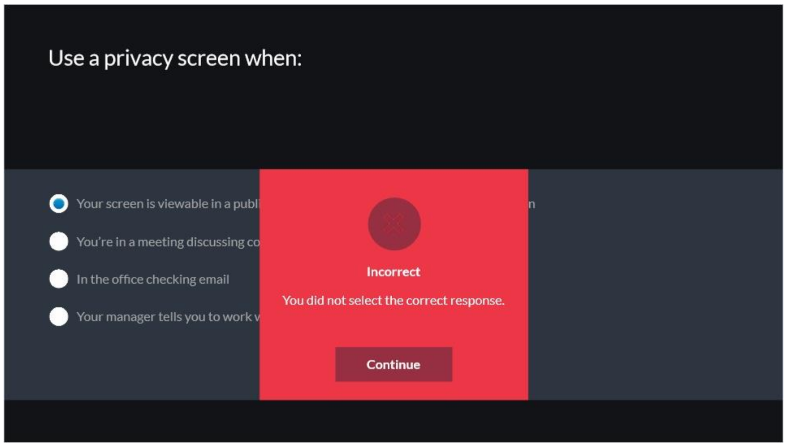
○ In the office checking email

○ Your manager tells you to work v

Correct

That's right! You selected the correct response.

Incorrect (Slide Layer)



Use a privacy screen when:

● Your screen is viewable in a publ n

○ You're in a meeting discussing co

○ In the office checking email

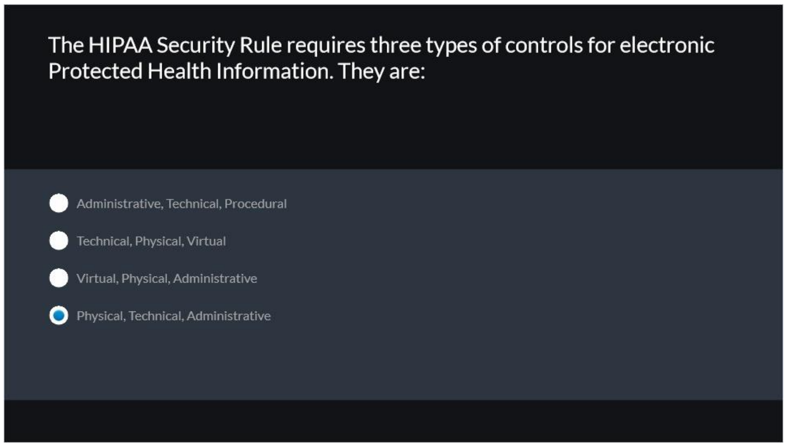
○ Your manager tells you to work v

Incorrect

You did not select the correct response.

Q2.2 MULTIPLE CHOICE QUESTION

(Multiple Choice, 10 points, 1 attempt permitted)



The HIPAA Security Rule requires three types of controls for electronic Protected Health Information. They are:

○ Administrative, Technical, Procedural

○ Technical, Physical, Virtual

○ Virtual, Physical, Administrative

● Physical, Technical, Administrative

Correct	Choice
	Administrative, Technical, Procedural
	Technical, Physical, Virtual
	Virtual, Physical, Administrative
X	Physical, Technical, Administrative

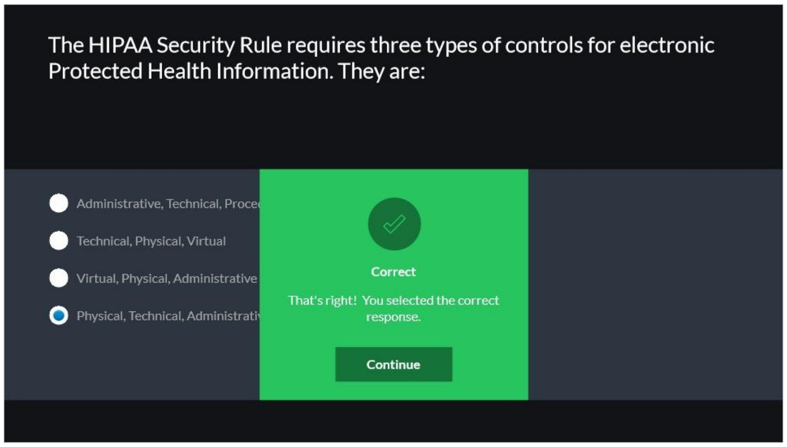
Feedback when correct:

That's right! You selected the correct response.

Feedback when incorrect:

You did not select the correct response.

Correct (Slide Layer)



The HIPAA Security Rule requires three types of controls for electronic Protected Health Information. They are:

○ Administrative, Technical, Proce

○ Technical, Physical, Virtual

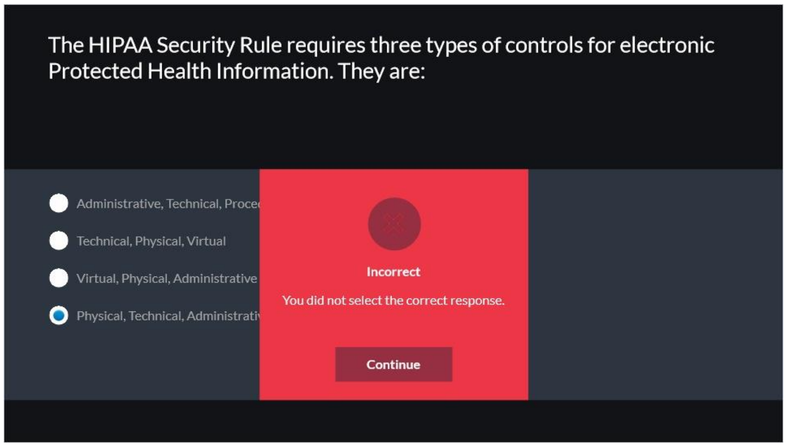
○ Virtual, Physical, Administrative

● Physical, Technical, Administrati

Correct

That's right! You selected the correct response.

Incorrect (Slide Layer)



The HIPAA Security Rule requires three types of controls for electronic Protected Health Information. They are:

○ Administrative, Technical, Proce

○ Technical, Physical, Virtual

○ Virtual, Physical, Administrative

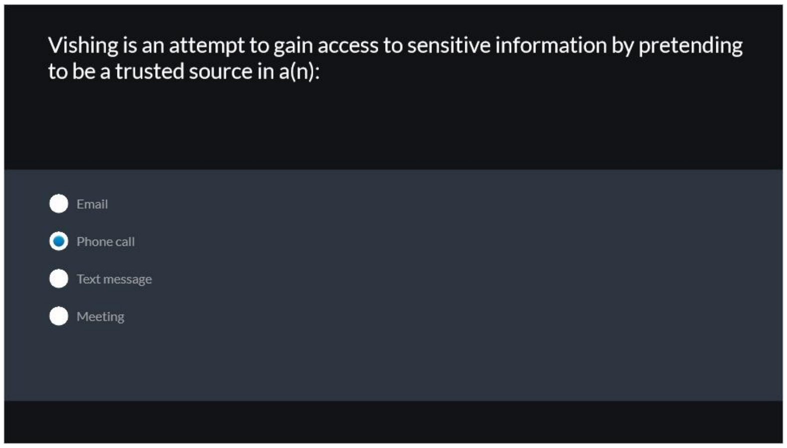
● Physical, Technical, Administrati

Incorrect

You did not select the correct response.

Q2.3 MULTIPLE CHOICE QUESTION

(Multiple Choice, 10 points, 1 attempt permitted)



Vishing is an attempt to gain access to sensitive information by pretending to be a trusted source in a(n):

○ Email

● Phone call

○ Text message

○ Meeting

Correct	Choice
	Email
X	Phone call
	Text message
	Meeting

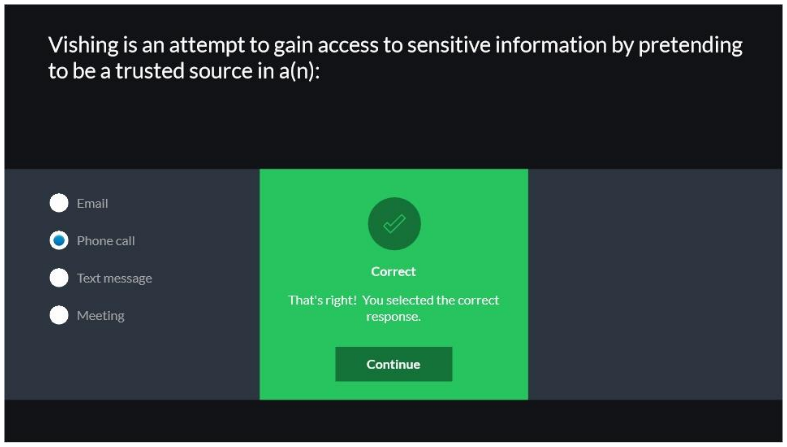
Feedback when correct:

That's right! You selected the correct response.

Feedback when incorrect:

You did not select the correct response.

Correct (Slide Layer)



Vishing is an attempt to gain access to sensitive information by pretending to be a trusted source in a(n):

○ Email

● Phone call

○ Text message

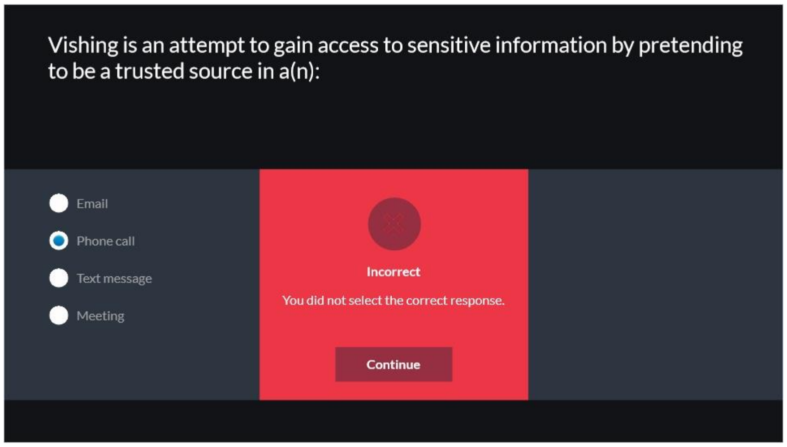
○ Meeting

Correct

That's right! You selected the correct response.

Continue

Incorrect (Slide Layer)



Vishing is an attempt to gain access to sensitive information by pretending to be a trusted source in a(n):

○ Email

● Phone call

○ Text message

○ Meeting

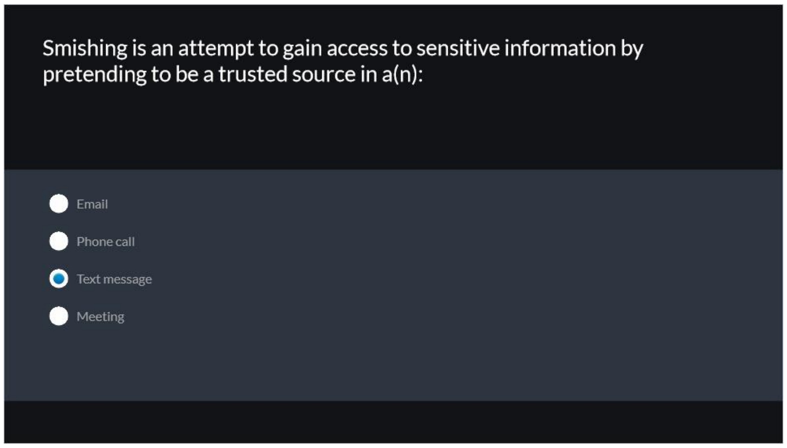
Incorrect

You did not select the correct response.

Continue

Q2.4 MULTIPLE CHOICE QUESTION

(Multiple Choice, 10 points, 1 attempt permitted)



Smishing is an attempt to gain access to sensitive information by pretending to be a trusted source in a(n):

○ Email

○ Phone call

● Text message

○ Meeting

Correct	Choice
	Email
	Phone call
X	Text message
	Meeting

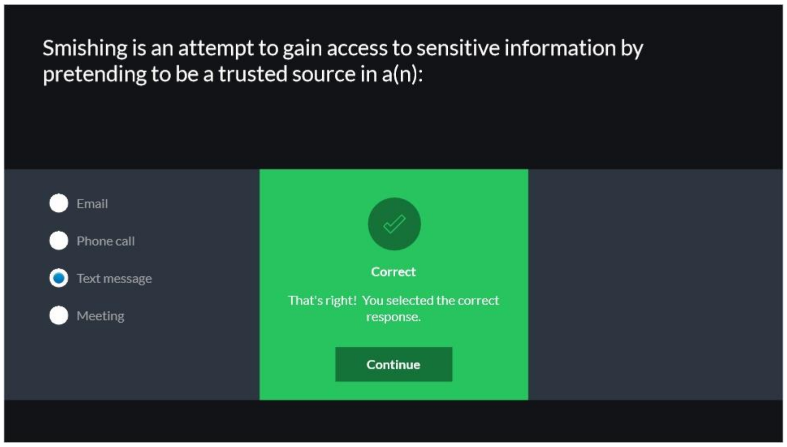
Feedback when correct:

That's right! You selected the correct response.

Feedback when incorrect:

You did not select the correct response.

Correct (Slide Layer)



Smishing is an attempt to gain access to sensitive information by pretending to be a trusted source in a(n):

○ Email

○ Phone call

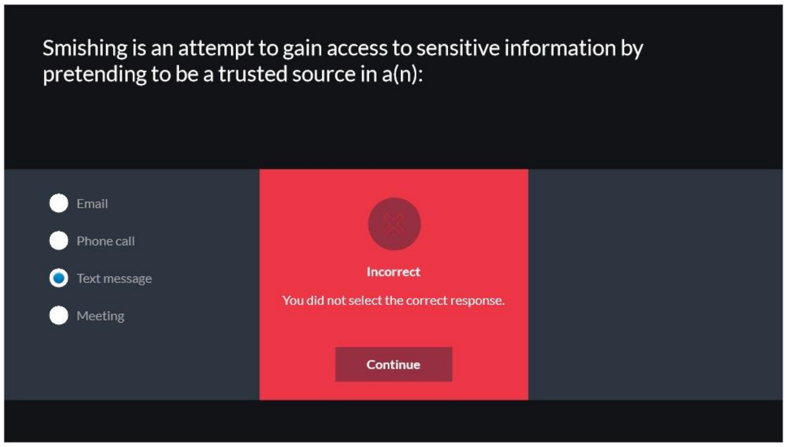
● Text message

○ Meeting

Correct

That's right! You selected the correct response.

Incorrect (Slide Layer)



Smishing is an attempt to gain access to sensitive information by pretending to be a trusted source in a(n):

○ Email

○ Phone call

● Text message

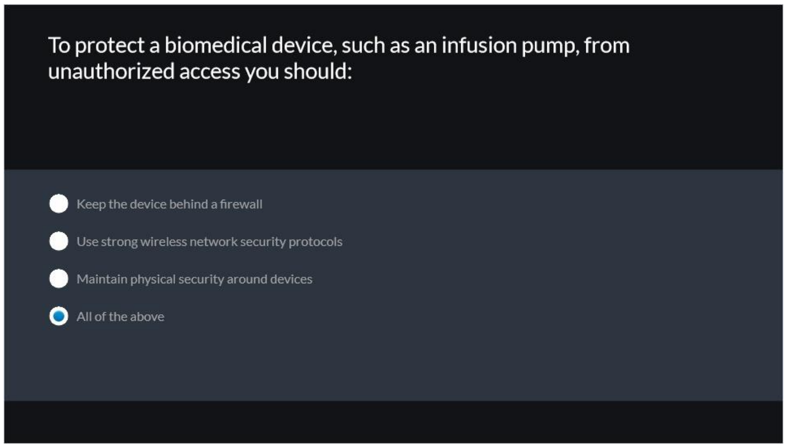
○ Meeting

Incorrect

You did not select the correct response.

Q2.5 MULTIPLE CHOICE QUESTION

(Multiple Choice, 10 points, 1 attempt permitted)



To protect a biomedical device, such as an infusion pump, from unauthorized access you should:

○ Keep the device behind a firewall

○ Use strong wireless network security protocols

○ Maintain physical security around devices

● All of the above

Correct	Choice
	Keep the device behind a firewall
	Use strong wireless network security protocols
	Maintain physical security around devices
X	All of the above

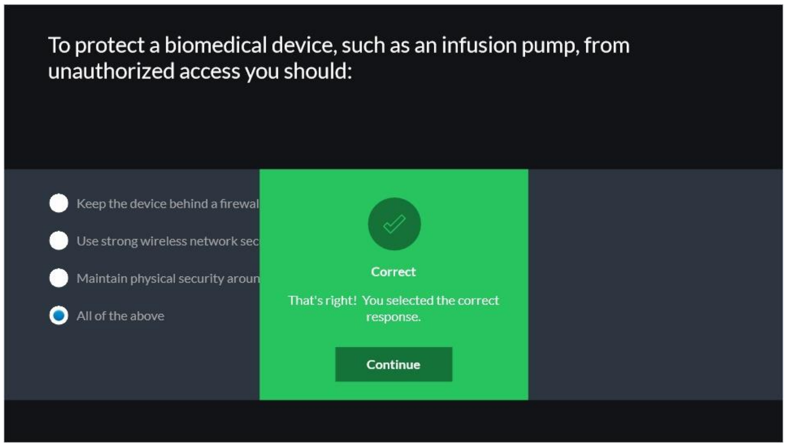
Feedback when correct:

That's right! You selected the correct response.

Feedback when incorrect:

You did not select the correct response.

Correct (Slide Layer)



To protect a biomedical device, such as an infusion pump, from unauthorized access you should:

○ Keep the device behind a firewal

○ Use strong wireless network sec

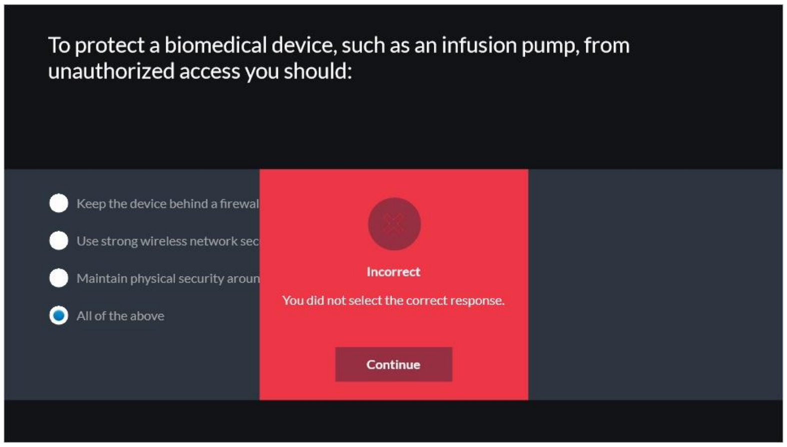
○ Maintain physical security aroun

● All of the above

Correct

That's right! You selected the correct response.

Incorrect (Slide Layer)



To protect a biomedical device, such as an infusion pump, from unauthorized access you should:

○ Keep the device behind a firewal

○ Use strong wireless network sec

○ Maintain physical security aroun

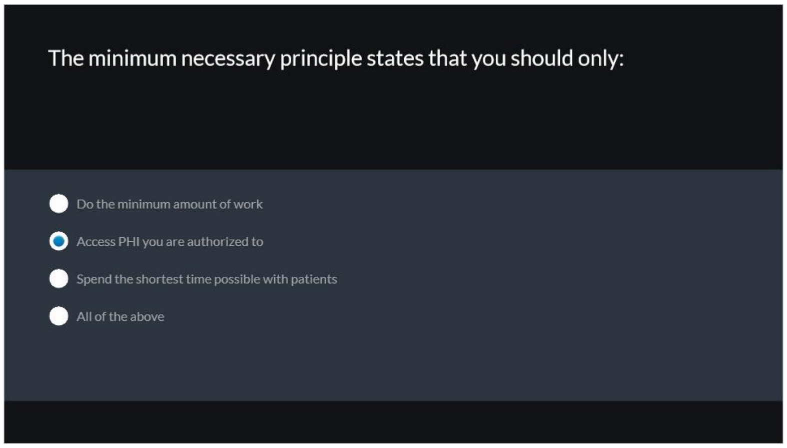
● All of the above

Incorrect

You did not select the correct response.

Q2.6 MULTIPLE CHOICE QUESTION

(Multiple Choice, 10 points, 1 attempt permitted)



The minimum necessary principle states that you should only:

○ Do the minimum amount of work

● Access PHI you are authorized to

○ Spend the shortest time possible with patients

○ All of the above

Correct	Choice
	Do the minimum amount of work
X	Access PHI you are authorized to
	Spend the shortest time possible with patients
	All of the above

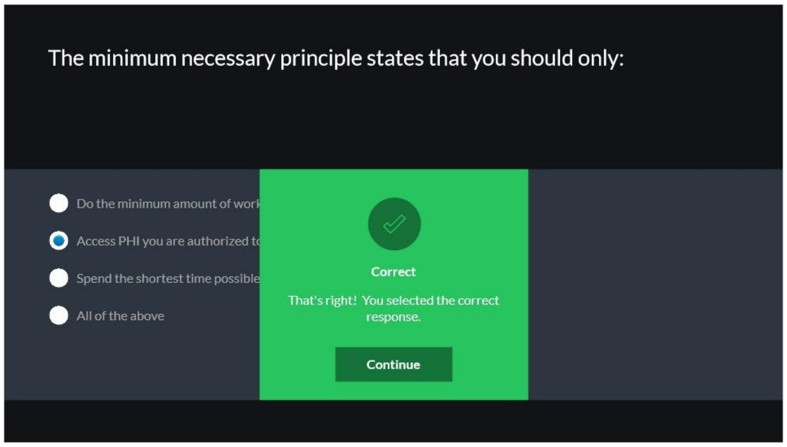
Feedback when correct:

That's right! You selected the correct response.

Feedback when incorrect:

You did not select the correct response.

Correct (Slide Layer)



The minimum necessary principle states that you should only:

○ Do the minimum amount of work

● Access PHI you are authorized to

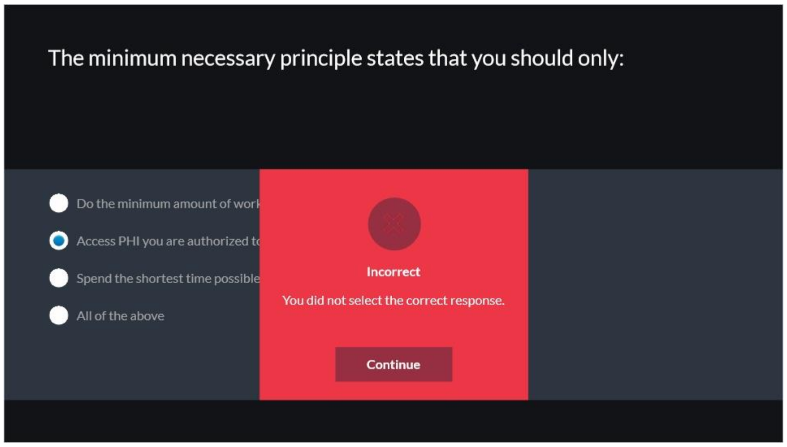
○ Spend the shortest time possible

○ All of the above

Correct

That's right! You selected the correct response.

Incorrect (Slide Layer)



The minimum necessary principle states that you should only:

○ Do the minimum amount of work

● Access PHI you are authorized to

○ Spend the shortest time possible

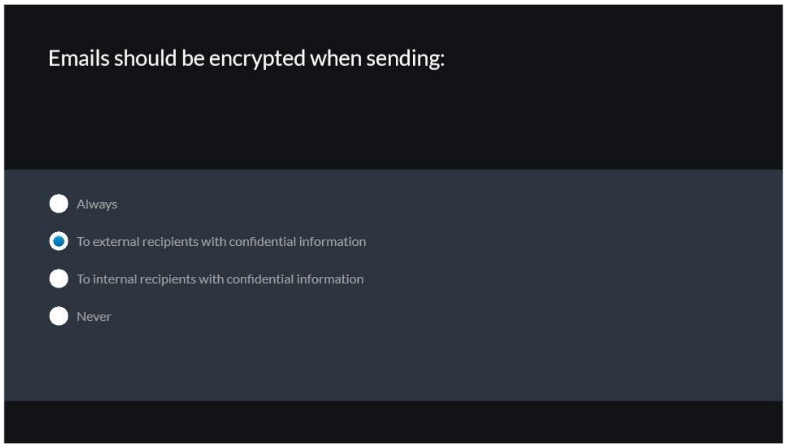
○ All of the above

Incorrect

You did not select the correct response.

Q2.7 MULTIPLE CHOICE QUESTION

(Multiple Choice, 10 points, 1 attempt permitted)



Emails should be encrypted when sending:

○ Always

● To external recipients with confidential information

○ To internal recipients with confidential information

○ Never

Correct	Choice
	Always
X	To external recipients with confidential information
	To internal recipients with confidential information
	Never

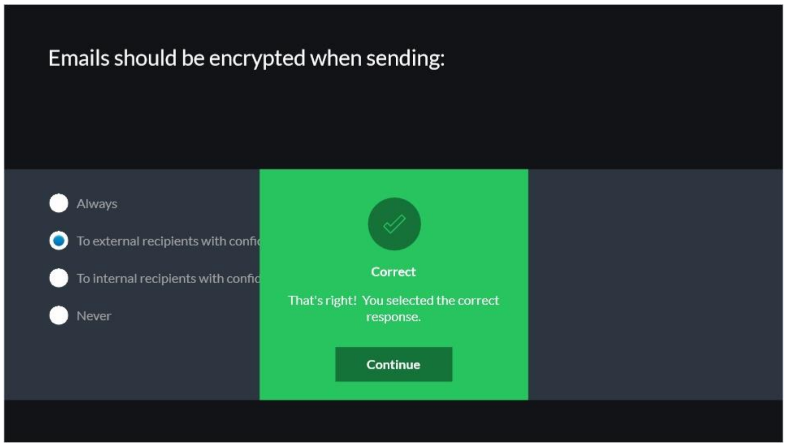
Feedback when correct:

That's right! You selected the correct response.

Feedback when incorrect:

You did not select the correct response.

Correct (Slide Layer)



Emails should be encrypted when sending:

○ Always

● To external recipients with confic

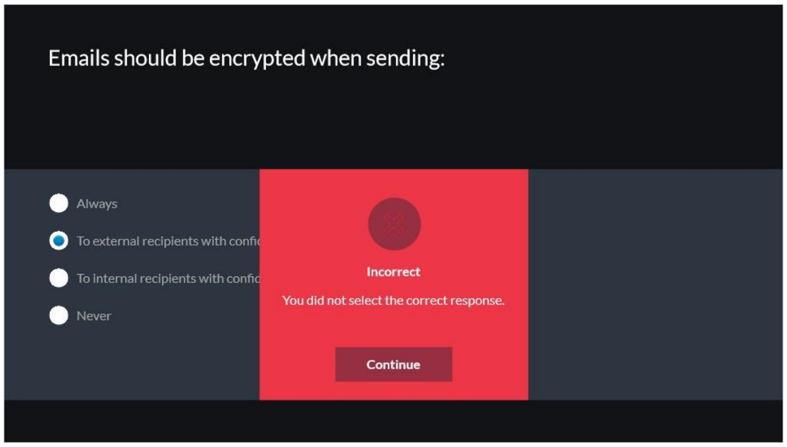
○ To internal recipients with confic

○ Never

Correct

That's right! You selected the correct response.

Incorrect (Slide Layer)



Emails should be encrypted when sending:

○ Always

● To external recipients with confic

○ To internal recipients with confic

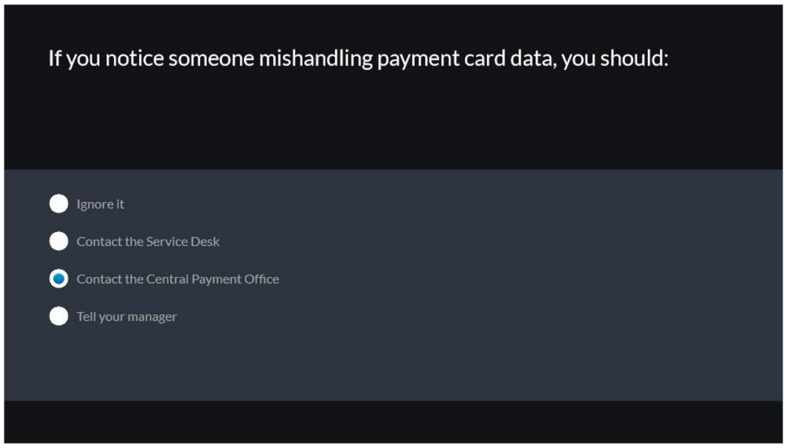
○ Never

Incorrect

You did not select the correct response.

Q2.8 MULTIPLE CHOICE QUESTION

(Multiple Choice, 10 points, 1 attempt permitted)



If you notice someone mishandling payment card data, you should:

○ Ignore it

○ Contact the Service Desk

● Contact the Central Payment Office

○ Tell your manager

Correct	Choice
	Ignore it
	Contact the Service Desk
X	Contact the Central Payment Office
	Tell your manager

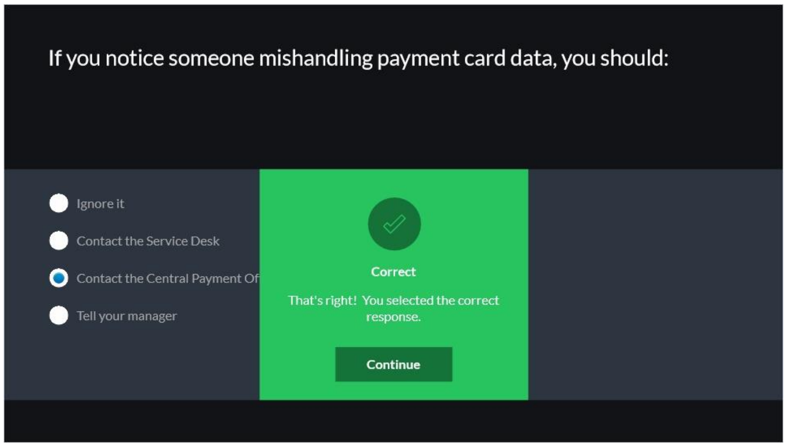
Feedback when correct:

That's right! You selected the correct response.

Feedback when incorrect:

You did not select the correct response.

Correct (Slide Layer)



If you notice someone mishandling payment card data, you should:

○ Ignore it

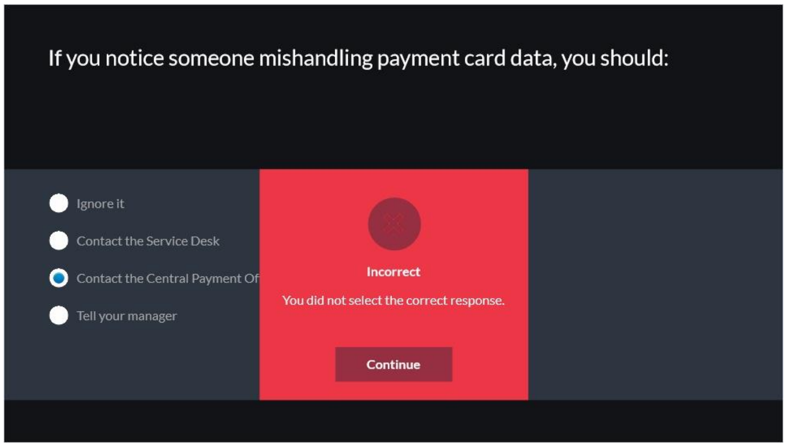
○ Contact the Service Desk

● Contact the Central Payment Of

○ Tell your manager

That's right! You selected the correct response.

Incorrect (Slide Layer)



If you notice someone mishandling payment card data, you should:

○ Ignore it

○ Contact the Service Desk

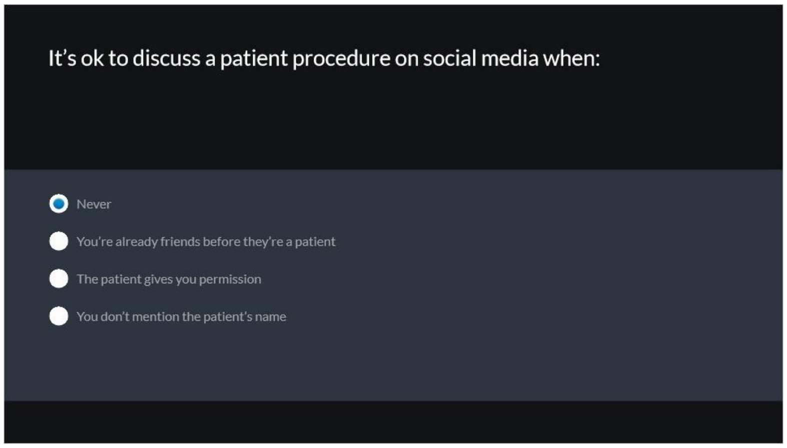
● Contact the Central Payment Of

○ Tell your manager

You did not select the correct response.

Q2.9 MULTIPLE CHOICE QUESTION

(Multiple Choice, 10 points, 1 attempt permitted)



It’s ok to discuss a patient procedure on social media when:

- ● Never
- ○ You’re already friends before they’re a patient
- ○ The patient gives you permission
- ○ You don’t mention the patient’s name

Correct	Choice
X	Never
	You’re already friends before they’re a patient
	The patient gives you permission
	You don’t mention the patient’s name

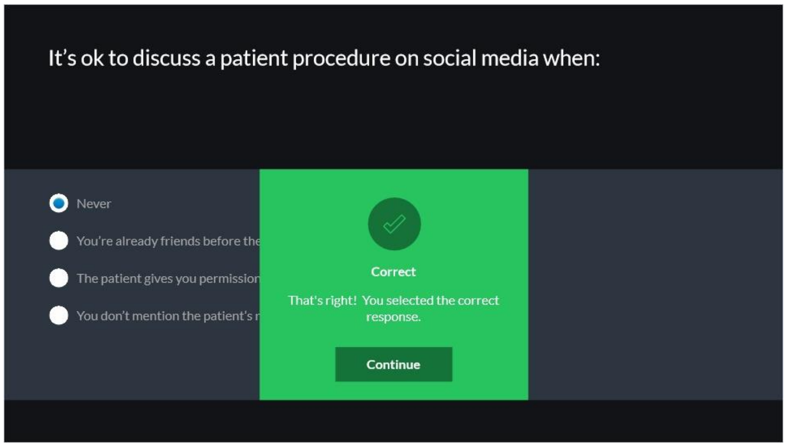
Feedback when correct:

That's right! You selected the correct response.

Feedback when incorrect:

You did not select the correct response.

Correct (Slide Layer)



It’s ok to discuss a patient procedure on social media when:

● Never

○ You’re already friends before the

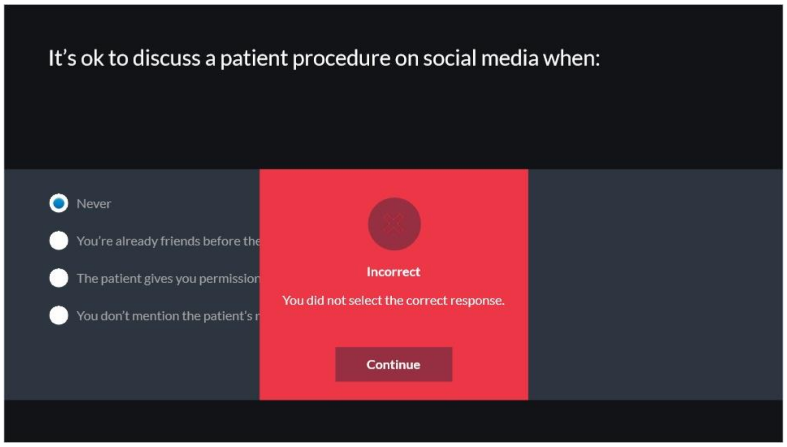
○ The patient gives you permission

○ You don’t mention the patient’s r

Correct

That's right! You selected the correct response.

Incorrect (Slide Layer)



It’s ok to discuss a patient procedure on social media when:

● Never

○ You’re already friends before the

○ The patient gives you permission

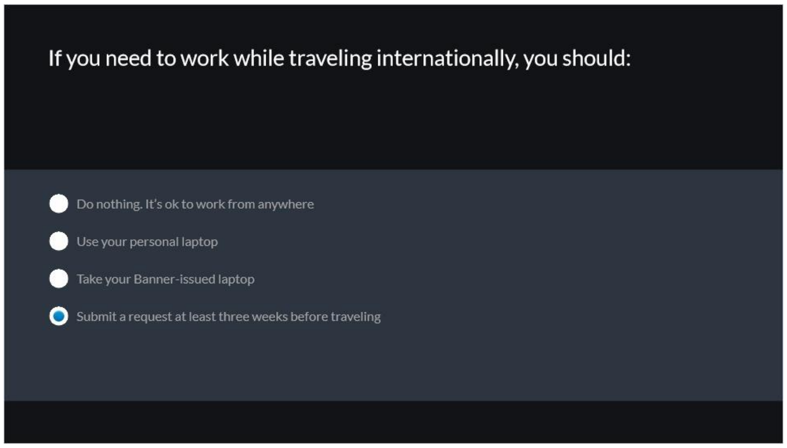
○ You don’t mention the patient’s r

Incorrect

You did not select the correct response.

Q2.10 MULTIPLE CHOICE QUESTION

(Multiple Choice, 10 points, 1 attempt permitted)



If you need to work while traveling internationally, you should:

○ Do nothing. It's ok to work from anywhere

○ Use your personal laptop

○ Take your Banner-issued laptop

● Submit a request at least three weeks before traveling

Correct	Choice
	Do nothing. It’s ok to work from anywhere
	Use your personal laptop
	Take your Banner-issued laptop
X	Submit a request at least three weeks before traveling

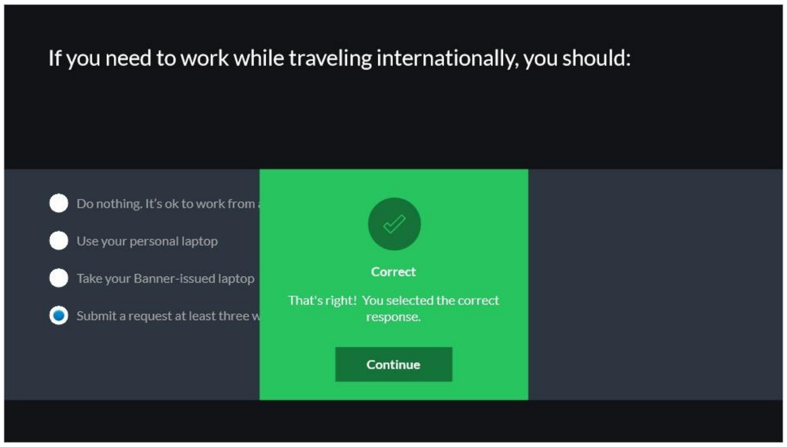
Feedback when correct:

That's right! You selected the correct response.

Feedback when incorrect:

You did not select the correct response.

Correct (Slide Layer)



If you need to work while traveling internationally, you should:

○ Do nothing. It's ok to work from a

○ Use your personal laptop

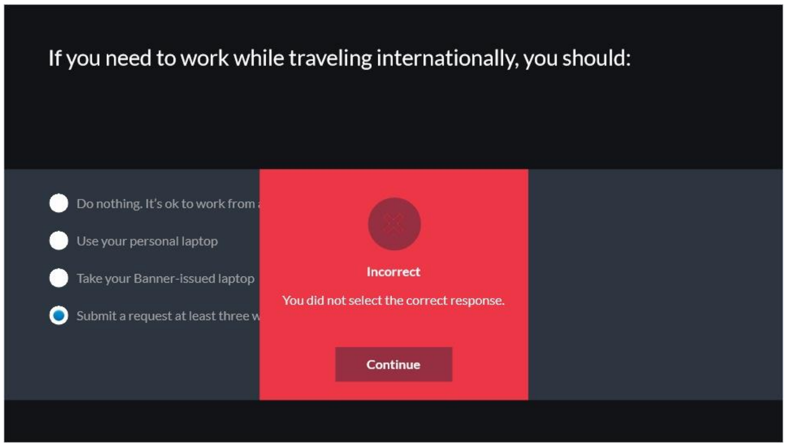
○ Take your Banner-issued laptop

● Submit a request at least three w

Correct

That's right! You selected the correct response.

Incorrect (Slide Layer)



If you need to work while traveling internationally, you should:

○ Do nothing. It's ok to work from a

○ Use your personal laptop

○ Take your Banner-issued laptop

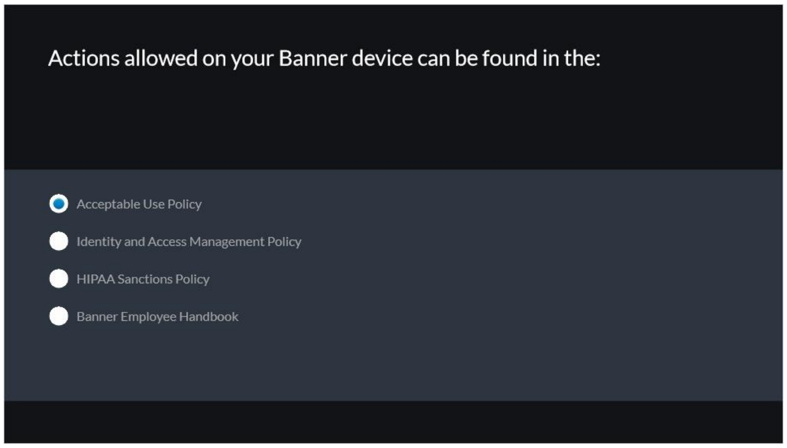
● Submit a request at least three w

Incorrect

You did not select the correct response.

Q2.11 MULTIPLE CHOICE QUESTION

(Multiple Choice, 10 points, 1 attempt permitted)



Actions allowed on your Banner device can be found in the:

● Acceptable Use Policy

○ Identity and Access Management Policy

○ HIPAA Sanctions Policy

○ Banner Employee Handbook

Correct	Choice
X	Acceptable Use Policy
	Identity and Access Management Policy
	HIPAA Sanctions Policy
	Banner Employee Handbook

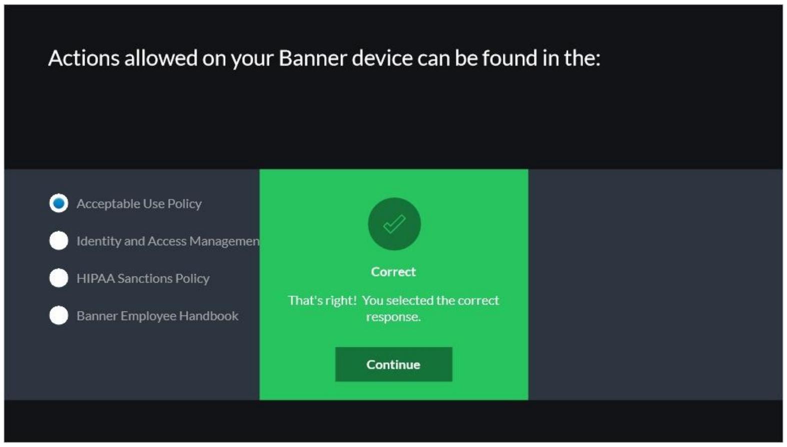
Feedback when correct:

That's right! You selected the correct response.

Feedback when incorrect:

You did not select the correct response.

Correct (Slide Layer)



Actions allowed on your Banner device can be found in the:

● Acceptable Use Policy

○ Identity and Access Managemen

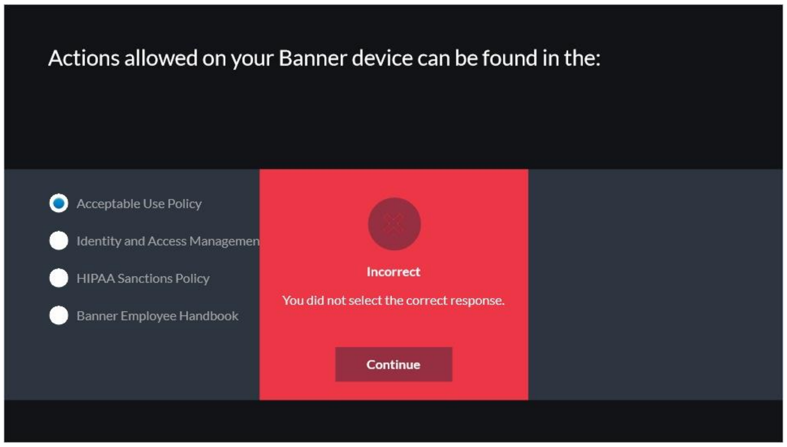
○ HIPAA Sanctions Policy

○ Banner Employee Handbook

Correct

That's right! You selected the correct response.

Incorrect (Slide Layer)



Actions allowed on your Banner device can be found in the:

● Acceptable Use Policy

○ Identity and Access Managemen

○ HIPAA Sanctions Policy

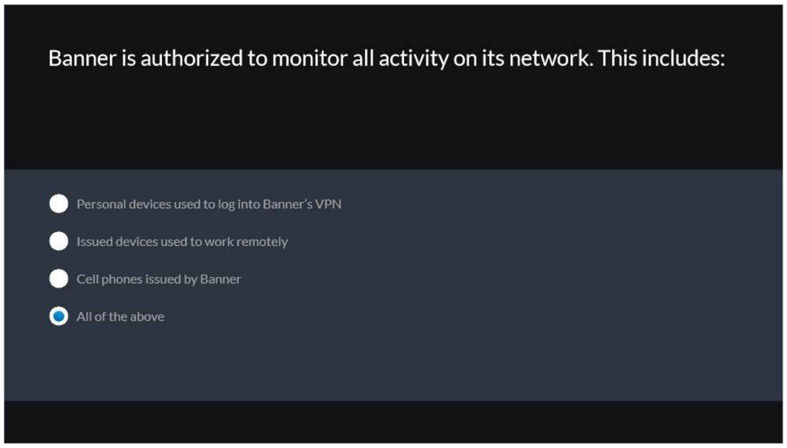
○ Banner Employee Handbook

Incorrect

You did not select the correct response.

Q2.12 MULTIPLE CHOICE QUESTION

(Multiple Choice, 10 points, 1 attempt permitted)



Banner is authorized to monitor all activity on its network. This includes:

○ Personal devices used to log into Banner’s VPN

○ Issued devices used to work remotely

○ Cell phones issued by Banner

● All of the above

Correct	Choice
	Personal devices used to log into Banner’s VPN
	Issued devices used to work remotely
	Cell phones issued by Banner
X	All of the above

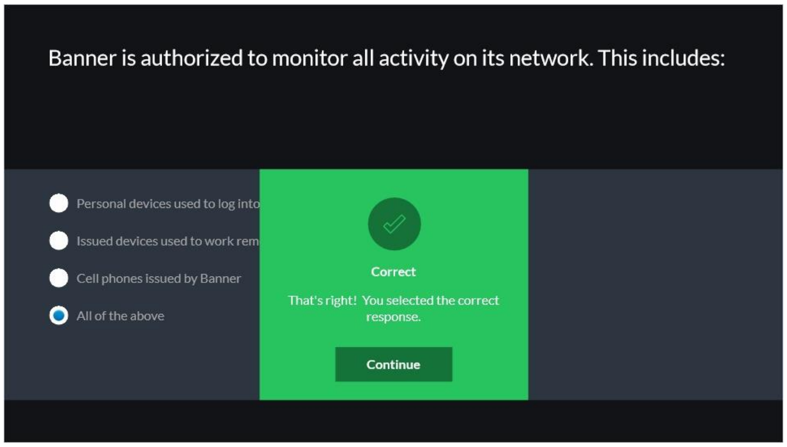
Feedback when correct:

That's right! You selected the correct response.

Feedback when incorrect:

You did not select the correct response.

Correct (Slide Layer)



Banner is authorized to monitor all activity on its network. This includes:

○ Personal devices used to log into

○ Issued devices used to work rem

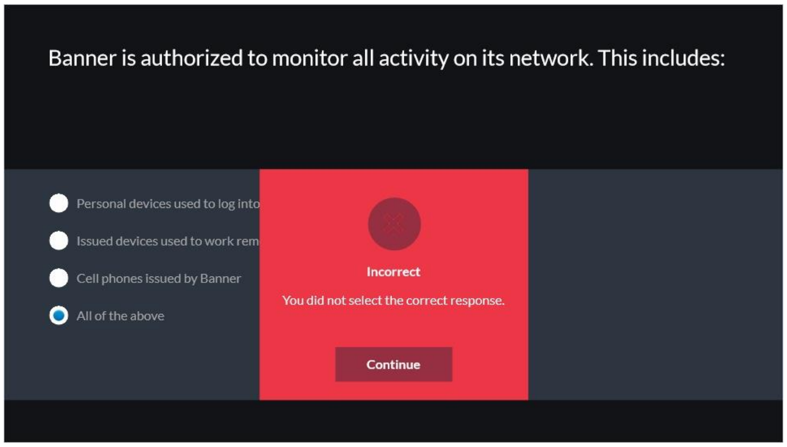
○ Cell phones issued by Banner

● All of the above

Correct

That's right! You selected the correct response.

Incorrect (Slide Layer)



Banner is authorized to monitor all activity on its network. This includes:

○ Personal devices used to log into

○ Issued devices used to work rem

○ Cell phones issued by Banner

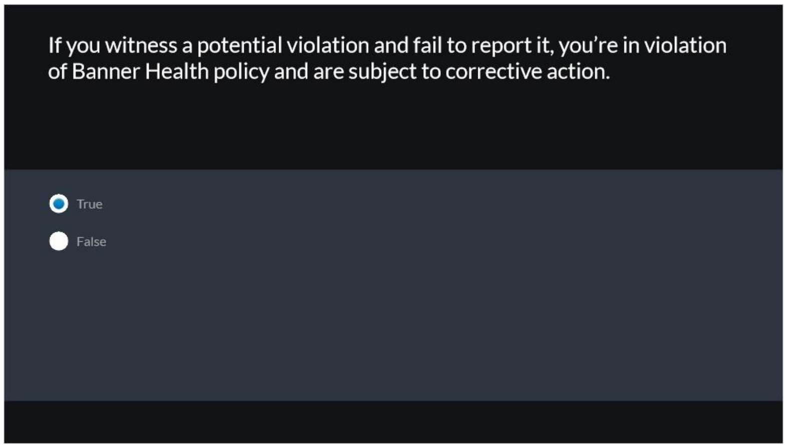
● All of the above

Incorrect

You did not select the correct response.

Q2.13 MULTIPLE CHOICE QUESTION

(Multiple Choice, 10 points, 1 attempt permitted)



If you witness a potential violation and fail to report it, you're in violation of Banner Health policy and are subject to corrective action.

● True

○ False

Correct	Choice
X	True
	False

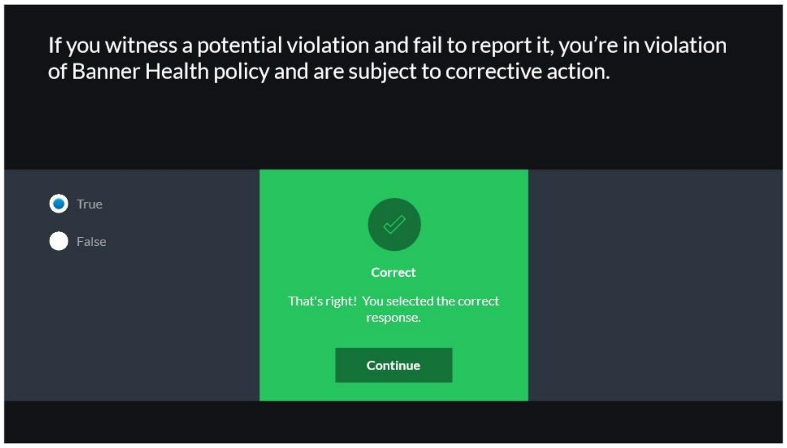
Feedback when correct:

That's right! You selected the correct response.

Feedback when incorrect:

You did not select the correct response.

Correct (Slide Layer)



If you witness a potential violation and fail to report it, you're in violation of Banner Health policy and are subject to corrective action.

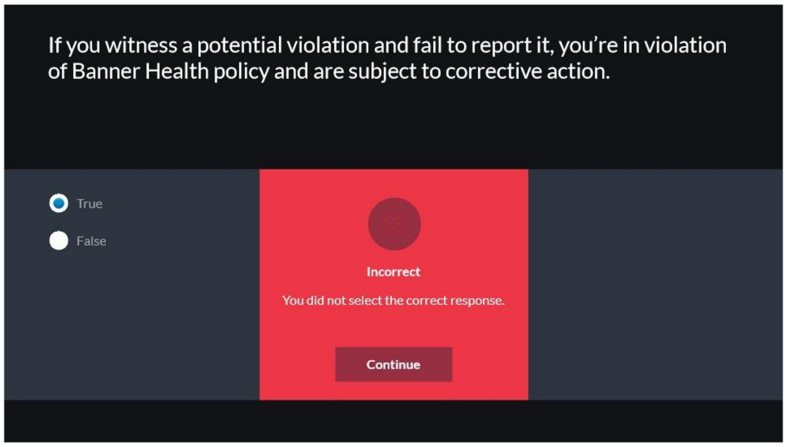
● True

○ False

Correct

That's right! You selected the correct response.

Incorrect (Slide Layer)



If you witness a potential violation and fail to report it, you're in violation of Banner Health policy and are subject to corrective action.

● True

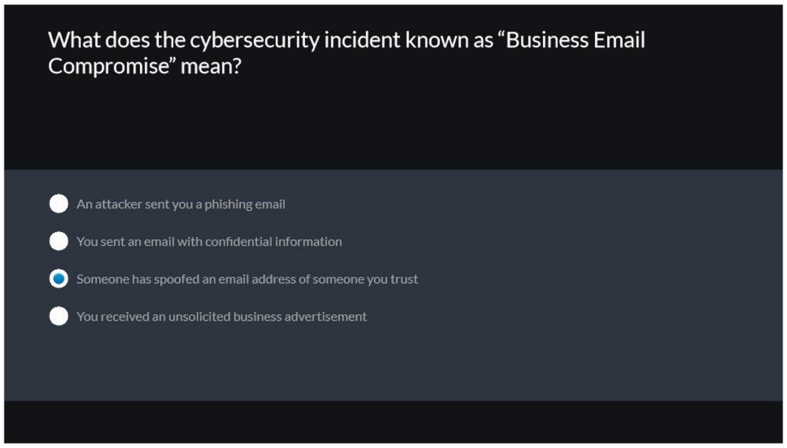
○ False

Incorrect

You did not select the correct response.

Q2.14 MULTIPLE CHOICE QUESTION

(Multiple Choice, 10 points, 1 attempt permitted)



What does the cybersecurity incident known as "Business Email Compromise" mean?

○ An attacker sent you a phishing email

○ You sent an email with confidential information

● Someone has spoofed an email address of someone you trust

○ You received an unsolicited business advertisement

Correct	Choice
	An attacker sent you a phishing email
	You sent an email with confidential information
X	Someone has spoofed an email address of someone you trust
	You received an unsolicited business advertisement

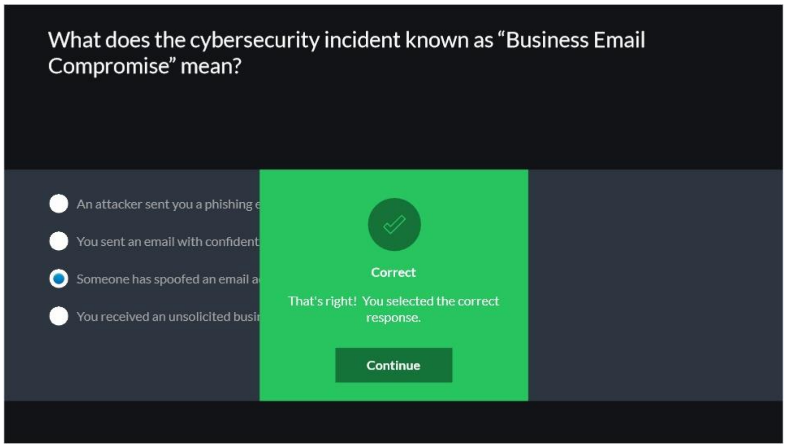
Feedback when correct:

That's right! You selected the correct response.

Feedback when incorrect:

You did not select the correct response.

Correct (Slide Layer)



What does the cybersecurity incident known as “Business Email Compromise” mean?

○ An attacker sent you a phishing e

○ You sent an email with confident

● Someone has spoofed an email a

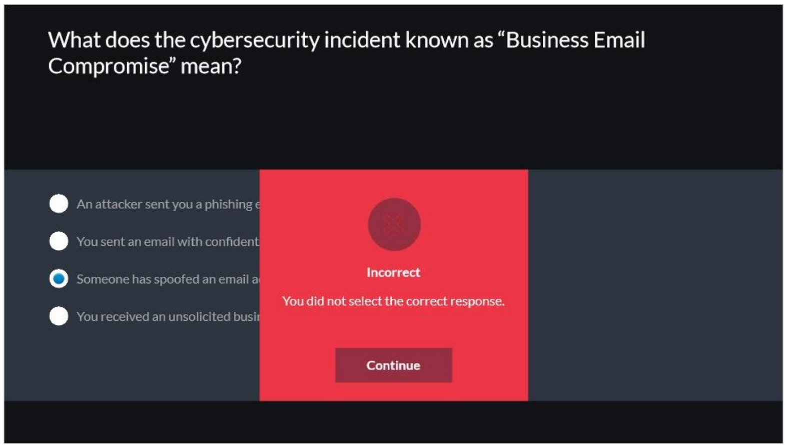
○ You received an unsolicited busi

Correct

That's right! You selected the correct response.

Continue

Incorrect (Slide Layer)



What does the cybersecurity incident known as “Business Email Compromise” mean?

○ An attacker sent you a phishing e

○ You sent an email with confident

● Someone has spoofed an email a

○ You received an unsolicited busi

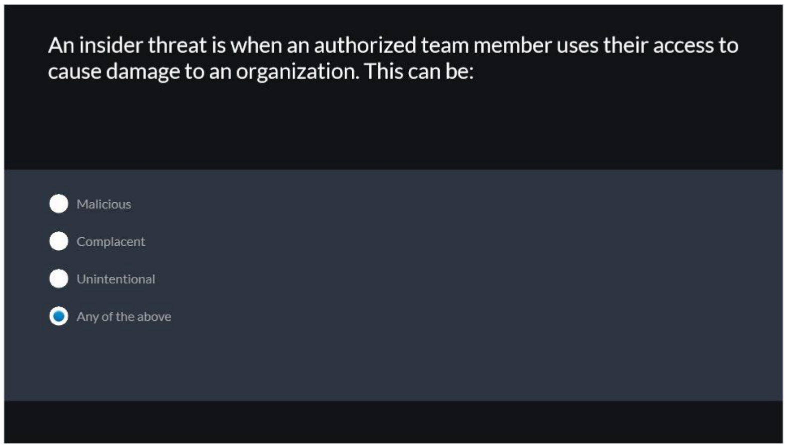
Incorrect

You did not select the correct response.

Continue

Q2.15 MULTIPLE CHOICE QUESTION

(Multiple Choice, 10 points, 1 attempt permitted)



An insider threat is when an authorized team member uses their access to cause damage to an organization. This can be:

○ Malicious

○ Complacent

○ Unintentional

● Any of the above

Correct	Choice
	Malicious
	Complacent
	Unintentional
X	Any of the above

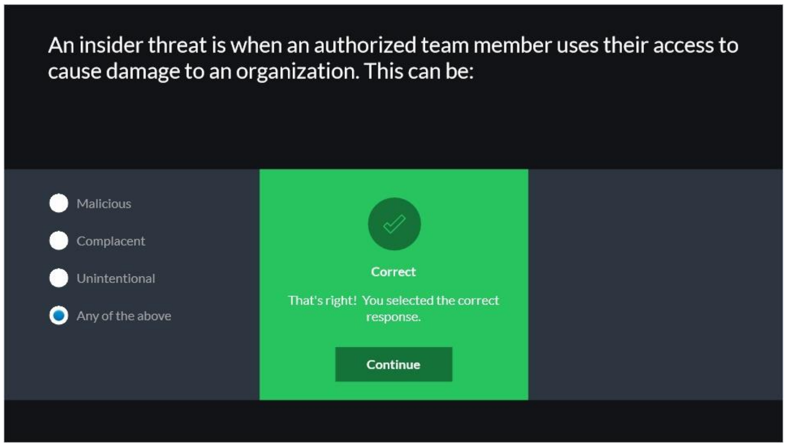
Feedback when correct:

That's right! You selected the correct response.

Feedback when incorrect:

You did not select the correct response.

Correct (Slide Layer)



An insider threat is when an authorized team member uses their access to cause damage to an organization. This can be:

○ Malicious

○ Complacent

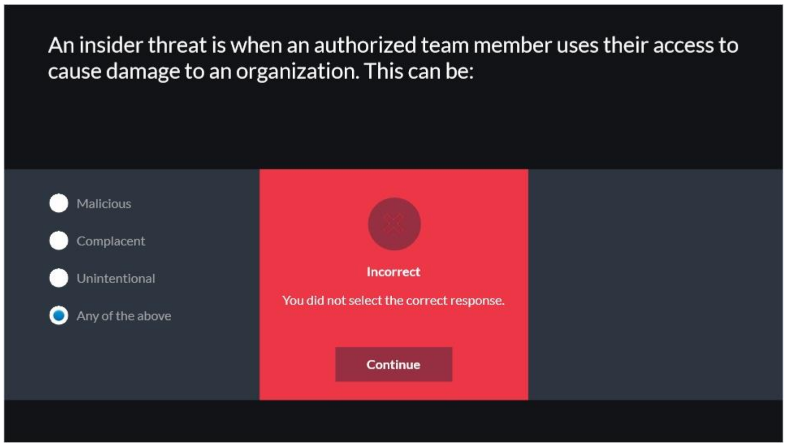
○ Unintentional

● Any of the above

Correct

That's right! You selected the correct response.

Incorrect (Slide Layer)



An insider threat is when an authorized team member uses their access to cause damage to an organization. This can be:

○ Malicious

○ Complacent

○ Unintentional

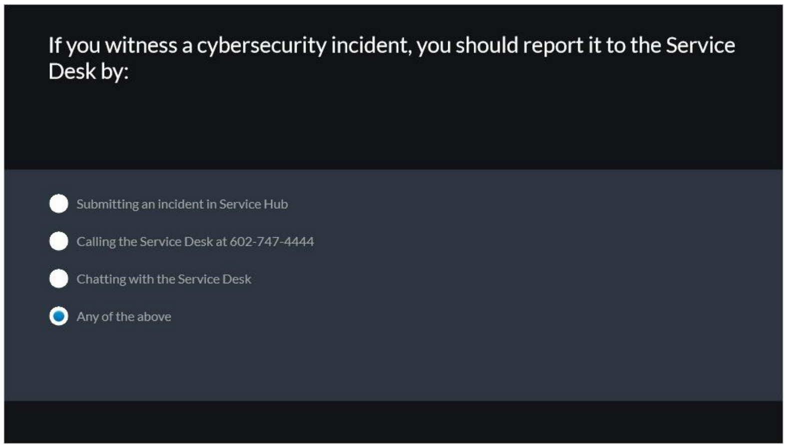
● Any of the above

Incorrect

You did not select the correct response.

Q2.16 MULTIPLE CHOICE QUESTION

(Multiple Choice, 10 points, 1 attempt permitted)



If you witness a cybersecurity incident, you should report it to the Service Desk by:

○ Submitting an incident in Service Hub

○ Calling the Service Desk at 602-747-4444

○ Chatting with the Service Desk

● Any of the above

Correct	Choice
	Submitting an incident in Service Hub
	Calling the Service Desk at 602-747-4444
	Chatting with the Service Desk
X	Any of the above

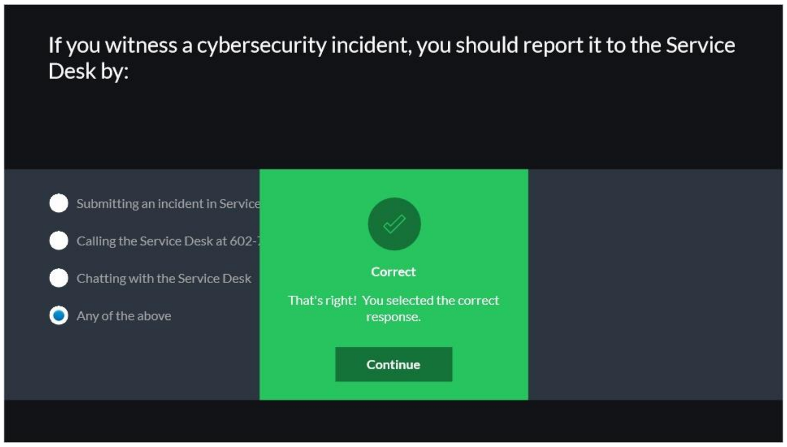
Feedback when correct:

That's right! You selected the correct response.

Feedback when incorrect:

You did not select the correct response.

Correct (Slide Layer)



If you witness a cybersecurity incident, you should report it to the Service Desk by:

○ Submitting an incident in Service

○ Calling the Service Desk at 602-7

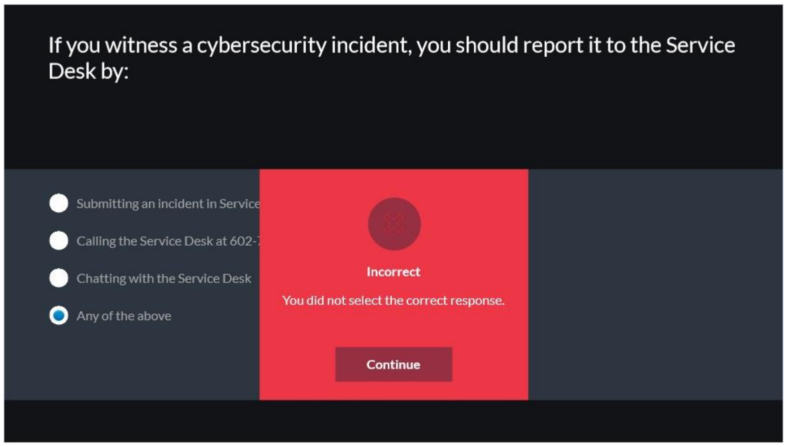
○ Chatting with the Service Desk

● Any of the above

Correct

That's right! You selected the correct response.

Incorrect (Slide Layer)



If you witness a cybersecurity incident, you should report it to the Service Desk by:

○ Submitting an incident in Service

○ Calling the Service Desk at 602-7

○ Chatting with the Service Desk

● Any of the above

Incorrect

You did not select the correct response.