Welcome to Bryant University's Security Awareness Training

Depending on your reading speed, this presentation will take approximately 12 minutes to complete.

This training is meant to familiarize you with common information security concerns and enable you to better protect university information.

Welcome to Bryant University's Security Awareness Training

After viewing this presentation you must take the training quiz on the last slide of this presentation to receive credit for the training.

Why is this important?

Think about everything you use your computer for in your personal life; banking, shopping, paying bills. Then consider how much of your personal information is involved in those transactions; social security number, name, address, financial information, etc.

Now imagine the amount of personal, sensitive information, Bryant University collects on students, faculty, staff, donors, perspective students and how that information is handled by you and members of your organization.

Where do you start?

Start by thinking about your role in the organization and task-related information you handle. Identify the resources and information assets (data, applications, systems, services, electronic files, etc.) that support critical functions of your organization. Identify the related risk to your organization and to the university if those critical functions or information assets become unavailable, are compromised or are inappropriately handled.

Remember, you first need to know what you have before you can secure it.

Secure what you have

There are simple steps you can take to ensure university information is protected.

Three factors are of primary importance:

Confidentiality – Protect sensitive information from unauthorized disclosure.

Integrity – Protect sensitive information from unauthorized modifications, and ensure the information is accurate and complete.

Availability – Ensure the information will be available when needed.

Secure information appropriately

Protect the data you are handling. While we want to have the most secure solutions possible, we also want them to be appropriate to the sensitivity of the data and the level of exposure.

Often people are granted more access than they need. Always keep in mind who is supposed to have access to what, and why? If someone asks you for access to information, make sure you confirm that they should have it.

- **Know where your data is stored**
- **Know what data is important**
- **Know your organization's guidelines for securing and disposing of data**
- **Don't keep what you don't need**
- **If you move data make sure its protection follows**

Tip: **Equip yourself with the knowledge of the University's data classification guidelines.**

When something doesn't seem right, take action

If you detect or suspect something isn't right, is not part of the normal workflow process or is just unusual, take action immediately. Don't take the chance of letting it become a disruptive event.

- **Monitor what's under your control**
- **Communicate your suspicions to your supervisor and/or the Helpdesk – REPORT IT**
- **Identify and mitigate risks that could lead to disruptive security events**
- **Think through the various scenarios that could happen, and prepare your response in advance**
- **Know what actions you can take to limit the impact if a disruption does occur**

What have we seen?

Analyzing the data from events we've seen, here's what we identify as the university's top three information security concerns.

1. **Exposure of confidential information (student, faculty, staff, parents, donors, perspective students); accidental or not**
2. **Unauthorized application or system access (email account takeover)**
3. **Loss of availability of systems and/or data (malware)**

Where are these threats coming from?

According to the data we've collected, email continues to be the cyber-criminals' vector of choice for distributing malicious software and phishing attacks. Social engineering is also a tool of choice for harvesting information relating to our university community.

1. **Phishing – email, phone, text, social media,**
2. **Malware – imbedded or downloaded in email attachments and links**
3. **Social Engineering – information we share online**

Does this email look suspicious?

From: Human Resources <hr.bryant.edu@gmail.com>
Sent: Thursday, July 25, 2019 11:14 AM
To: Richard Siedzik <rsiedzik@bryant.edu>
Subject: Bryant Alert

BRYANT HUMAN RESOURCES

PEOPLE FOCUSED
SOLUTIONS DRIVEN

Human Resources is committed to finding and providing solutions that achieve positive results efficiently, effectively, and in ways that continue to make us thrive as individuals and as an institution.

Richard,

We're designing a new compensation program and ***CONGRATULATIONS*** you are just one of a handful of employees selected to trial this new program at Bryant!

Due to the university's recent investment in mining stocks we're now able to send your monthly compensation to you in the form of gold or silver at a 1.0% to 2.0% higher market value than your monthly direct deposit. Click to ***like*** the program!

Because this program is only being trialed and not university-wide we ask that you keep this confidential and not share with others in the Bryant community. We in Human Resources assure you this email is legitimate and has been scanned by the Information Technology department for malicious links ***see tag at the end of this email***.

If you have specific questions Bryant's representative, Calum Lachlan, at the university's stock portfolio company, UnivPortInvest, will be happy to assist you.

(1 788.555.1234)

OPT into the trial and provide your current direct deposit banking information and the address where you would like the gold or silver shipped. ***Hurry,*** because the program is only open for enrollment for the next 24-hours. *Your personal data is safe with us!*

Melanie Cluley.
Human Resources
Bryant University

Content Scanned and Approved
Bryant Information Services

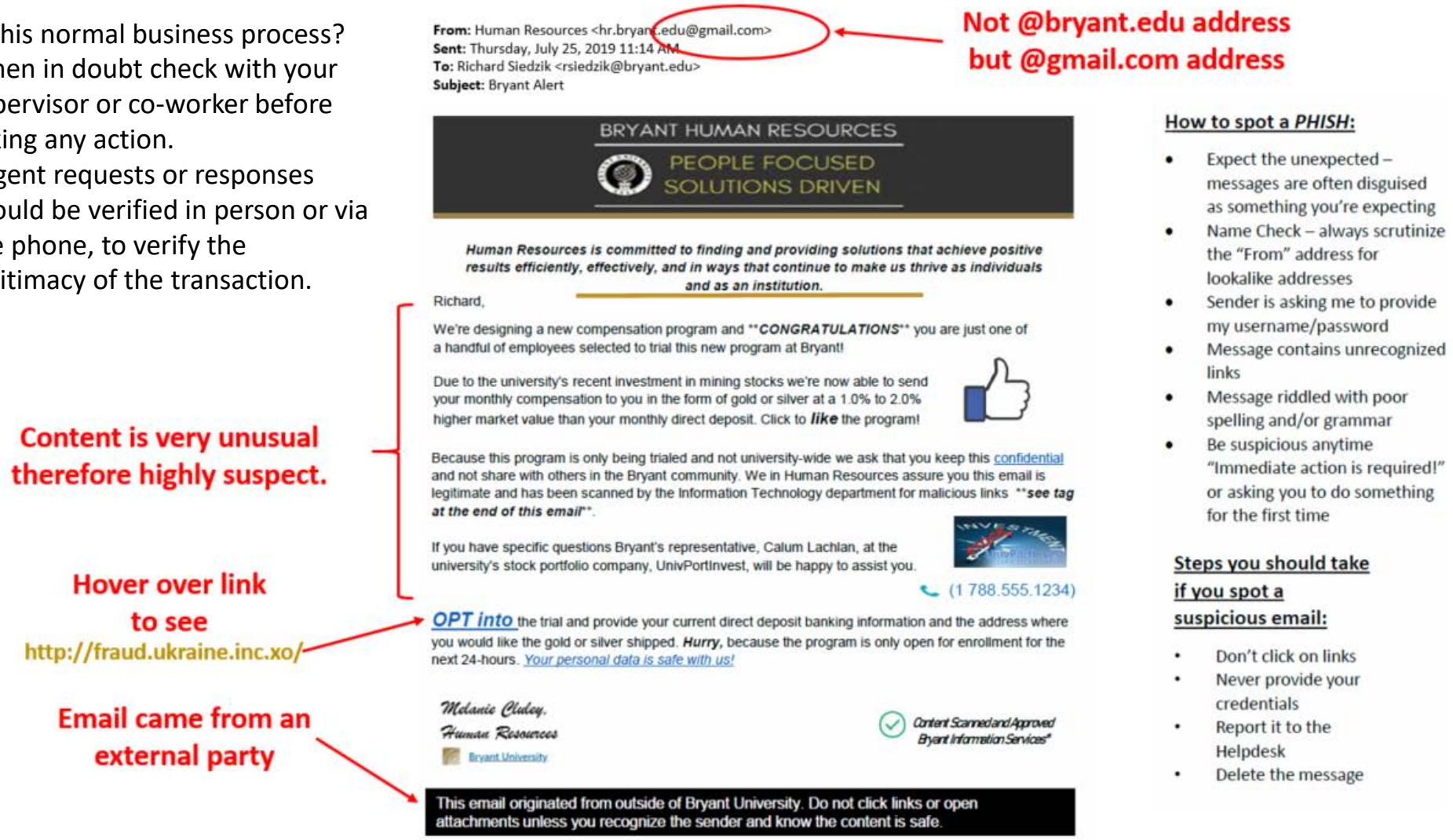
This email originated from outside of Bryant University. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Check out the next slide

Does this email look suspicious?

Ask yourself…

- Is this normal business process?
- When in doubt check with your supervisor or co-worker before taking any action.
- Urgent requests or responses should be verified in person or via the phone, to verify the legitimacy of the transaction.



How to spot a *PHISH*:

- Expect the unexpected – messages are often disguised as something you're expecting
- Name Check – always scrutinize the "From" address for lookalike addresses
- Sender is asking me to provide my username/password
- Message contains unrecognized links
- Message riddled with poor spelling and/or grammar
- Be suspicious anytime "Immediate action is required!" or asking you to do something for the first time

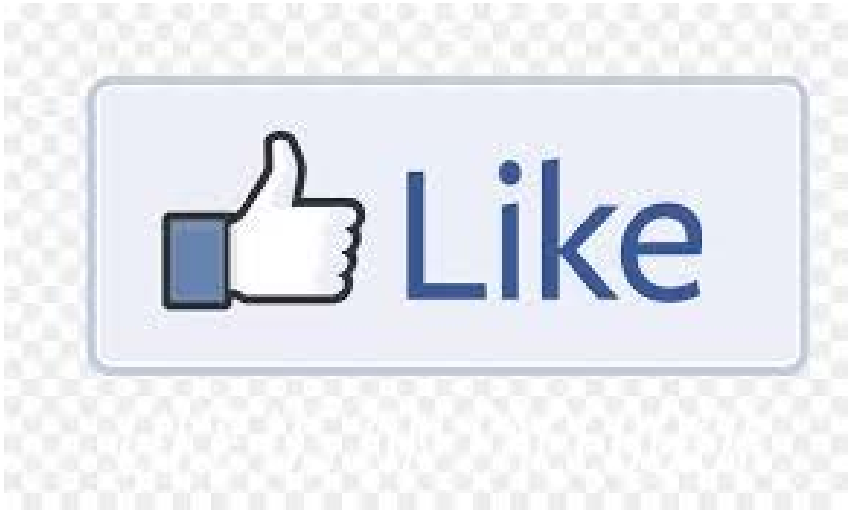
Steps you should take if you spot a suspicious email:

- Don't click on links
- Never provide your credentials
- Report it to the Helpdesk
- Delete the message

Data privacy at risk

Did you know a simple thing like clicking a ***Like*** button can put you at risk of leaking personal information if you haven't secured your application privacy setting correctly.

Click the Like Button to watch a short video of this actually happening to people.



See the big picture

When information security and data privacy are a frequent topic of discussion, well thought out, planned and employed cohesively within your organization, you're on the right path of protecting university information.

- **Security is a culture – help build that culture in your organization**
- **The best way to educate your staff about their role in security is to INVOLVE them**
- **Helping the university build upon its security framework and become more cyber-resilient is a shared long-term university commitment**

Safe Computing Practices

We need you to make a difference. No matter how safe the computer or sophisticated the technical controls in place, we rely on your actions and practices to safeguard the University's information. Therefore,…

- Equip yourself with the knowledge of security guidelines, practices, and procedures
- NEVER use your Bryant username and password for personal accounts
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly or contact the Helpdesk
- All "university business" correspondence should be sent from an official Bryant University email address
- Avoid opening attachments from an untrusted source
- Avoid clicking on links in an email from an untrusted source
- Avoid providing your user ID and password or other confidential information in an email or in a response to an email

Safe Computing Practices

Be the Difference

- Avoid storing personally identifiable information (PII) on local storage devices, e.g., desktop, laptop, USB, hand-held computers
- Follow university guidelines for storing any PII, confidential or sensitive data that you need for work process

How do you email sensitive data?

- Ensure that the recipient has a need for the sensitive data
- Follow university guidelines for securing and sending any PII, confidential or sensitive data in an email

Safe Computing Practices

What about social media?

- Review your privacy settings
- Think twice before you post
- Be selective about people you share with
- Closeout old accounts

And lastly…

- Look at the critical business processes – if not all - in your organization. Determine where there may be opportunity for discretion regarding a critical step or action, and then figure out how to remove that discretion and ensure sound practices are **ALWAYS** followed.

Tip: Click to check out this quick video on the risks of social media.

Contacts & Resources

To Report a Security Event
If you suspect a problem, contact the Information Security team infosec@bryant.edu or contact the Helpdesk helpdesk@bryant.edu

To Review Information Security Guidelines
Go to http://infosec.bryant.edu/guidelines.html

To Review Data Classification Guidelines
Go to http://infosec.bryant.edu/data_classification.html

To Review Data Storage Guidelines
Go to http://infosec.bryant.edu/storage.html

To Send Sensitive Information via Email
Go to https://my.bryant.edu/resources/help-desk/files/Secure%20Email.pdf

Questions & Concerns
To address any questions or concerns you may have, contact the Information Security team infosec@bryant.edu or contact the Helpdesk helpdesk@bryant.edu

Awareness Training Questions

Click here to take a three question quiz and receive credit for completing security awareness training. You must answer all three questions correctly.