INSURANCE BOARD
Partners in Protection

Cybersecurity Best Practices

Preventing measures, Managing Risk, Policy & Processes

Our insurance serves you so you can serve God.

ServeGod

INSURANCE BOARD
Partners in Protection

What is Cybersecurity?

- Defined as "the protection of computer systems and networks from attacks by malicious actors that may result in unauthorized information disclosure, theft of, or damage to hardware, software, or data..."
- Wherever there is technology, there needs to be cybersecurity.

Why is it Important?

- Implementing cybersecurity best practices is important for individuals as well as organizations of all sizes to protect personal, financial and sensitive information.
- For both government and private entities, developing and implementing tailored cybersecurity plans and processes is key to protecting and maintaining business operations.

INSURANCE BOARD
Partners in Protection

Why is this important to you

Board Member

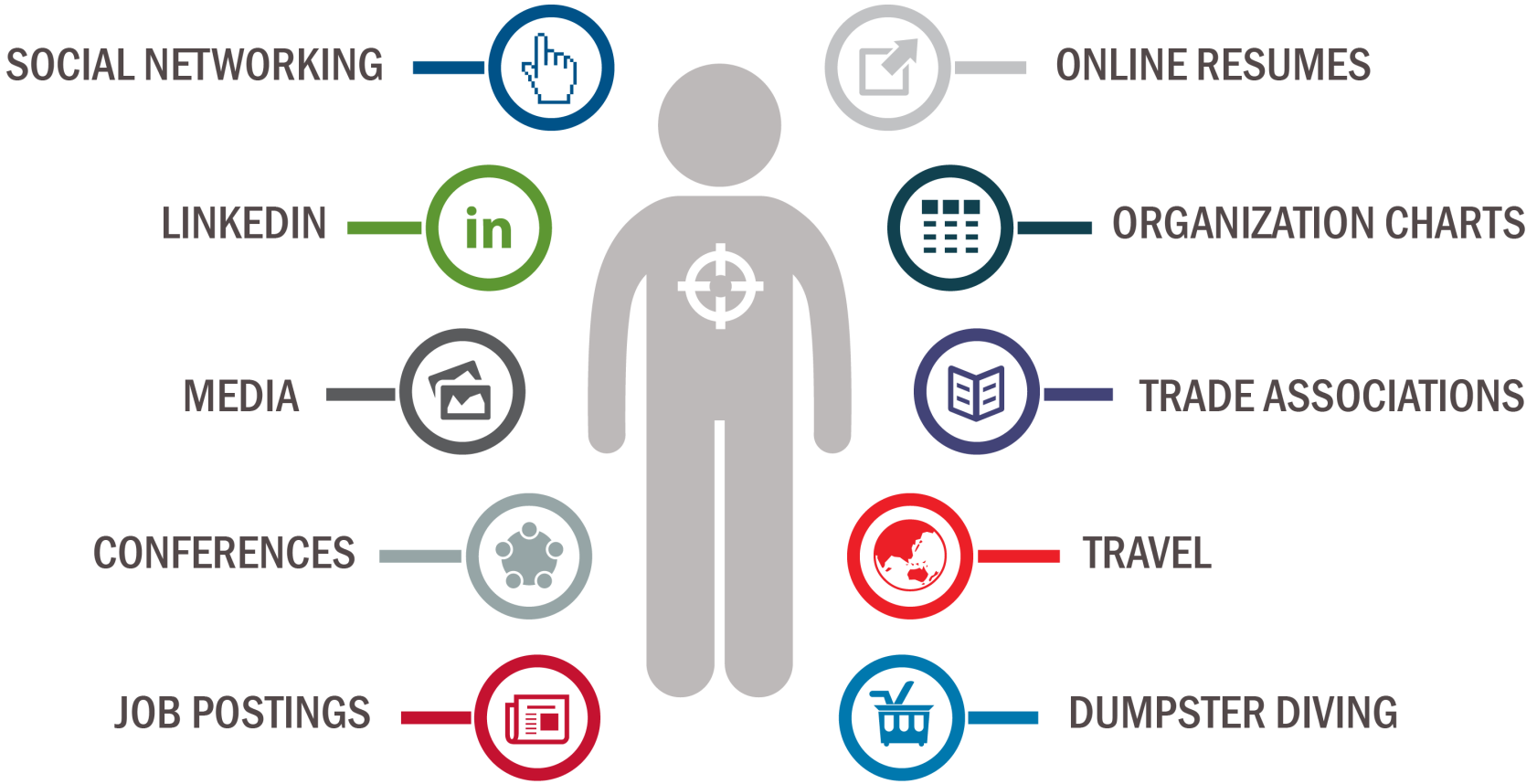
- Understand organization risk profile
- Ensure proactive risk assessments are conducted regularly
- Stay informed of emerging risk
- Allocate resources to address gaps

Leadership Role

- Know organizations risk profile
- Conduct proactive risk assessments
- Communicate to all applicable stakeholders emerging risks
- Identify and Request resources to address gaps

INSURANCE BOARD
Partners in Protection

How Are You Targeted



INSURANCE BOARD
Partners in Protection

Glossary of Terms

BEC Attack- Business Email Compromise- a form of phishing that occurs when a cybercriminal impersonates a legitimate source to trick employees into wiring money and sharing sensitive information.

Phishing- Soliciting private information from customers or members of a business, bank or other organization in an attempt to fool them into divulging confidential personal and financial information. People are lured into sharing usernames, passwords, account information or credit card numbers, usually by clicking on a link provided. See also Vishing.

Ransomware- A type of malware that holds the victim's data hostage and demands payment for the user to regain control.

Click here for more terms

INSURANCE BOARD
Partners in Protection

Business Email Compromise(BEC)

Common Attacks

False invoice schemes—Cybercriminals pretend to be business suppliers and request fund transfers to complete an invoice.

CEO fraud—Criminals pose as high-level executives to request wire transfers.

Account compromise—Cybercriminals hack into an executive or employee account to request invoice payments directly from vendors.

Attorney impersonation—Hackers impersonate a corporate lawyer or law firm to request an immediate transfer of funds.

Data theft—Criminals pose as HR professionals or employees in other functional roles to obtain personally identifiable information or tax statements from other employees or executives.

Our insurance serves you so you can serve God.

ServeGod

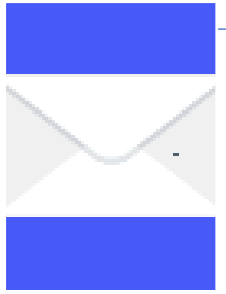
INSURANCE BOARD
Partners in Protection

Signs of BEC Attack

- Generic terms or lack of personalization
- Variations to email addresses or company websites
- Unfamiliar names or Images
- A sense of urgency or threatening language
- Requests to send personal or financial information

INSURANCE BOARD
Partners in Protection

Protecting Against BEC



Educate Employees

Implement effective payment protocols

Restrict access to sensitive data

Utilize security features

Have a plan

Our insurance serves you so you can serve God.

ServeGod

INSURANCE BOARD
Partners in Protection

Email Best Practices

Implement	Implement Employee Training
Improve	Improve Password Management
Enable	Enable Multifactor Authentication
Be	Be Aware of Phishing Emails
Avoid	Avoid Public Wi-Fi
Access	Access Email Only on Company Approved Devices
Utilize	Utilize Endpoint Protection Solutions
Log out	Log Out of Email Accounts
Back up	Back-Up Data Regularly

INSURANCE BOARD
Partners in Protection

Phishing and Social Engineering

What and How

Our insurance serves you so you can serve God.

ServeGod

INSURANCE BOARD
Partners in Protection

Phishing and Social Engineering

INSURANCE BOARD
Partners in Protection

How Can Phishing Affect You?

- If you fall victim to phishing, the attacker may gain personal information from you such as user credentials, financial information, social security numbers, etc.
- They can then use this information to access your accounts and impersonate you for malicious reasons including financial gain.
- An attacker may send an email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem.

How Can Phishing Affect Your Organization?

- An organization’s cybersecurity is as strong as their employees' knowledge of it.
- If an employee falls victim to a phishing email and compromises any information, the employee is putting the whole organization at risk.
- The attack may compromise the organization’s information and data.
- It may also compromise employee information, customer data, corporate intellectual property, and customer financial data.

Recognize and Report Phishing

PHISHING RED FLAGS:

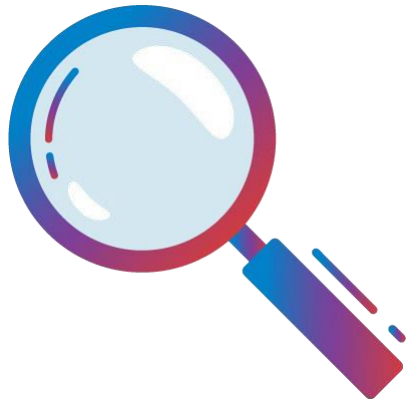
- **A tone that's urgent or makes you scared** *"Click this link immediately or your account will be closed"*

- **Bad spellings, bad grammar**
- **Requests to send personal info**
- **Sender email address doesn't match the company it's coming from**
  Ex: Amazon.com vs. Amaz0n.com
- **An email you weren't expecting**

Recognize and Report Phishing

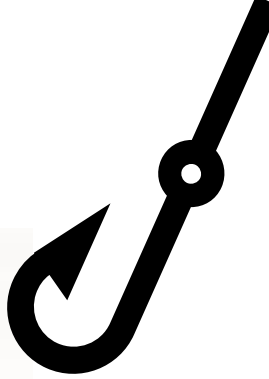
What to do?

- Do’s
  - Verify
  - Contact that person directly if it's someone you know
  - Report it to your IT department or email/phone provider
  - DELETE IT



- Don’t
  - Don't click any links
  - Don't click any attachments
  - Don't send personal info

INSURANCE BOARD
Partners in Protection



Time to Exercise

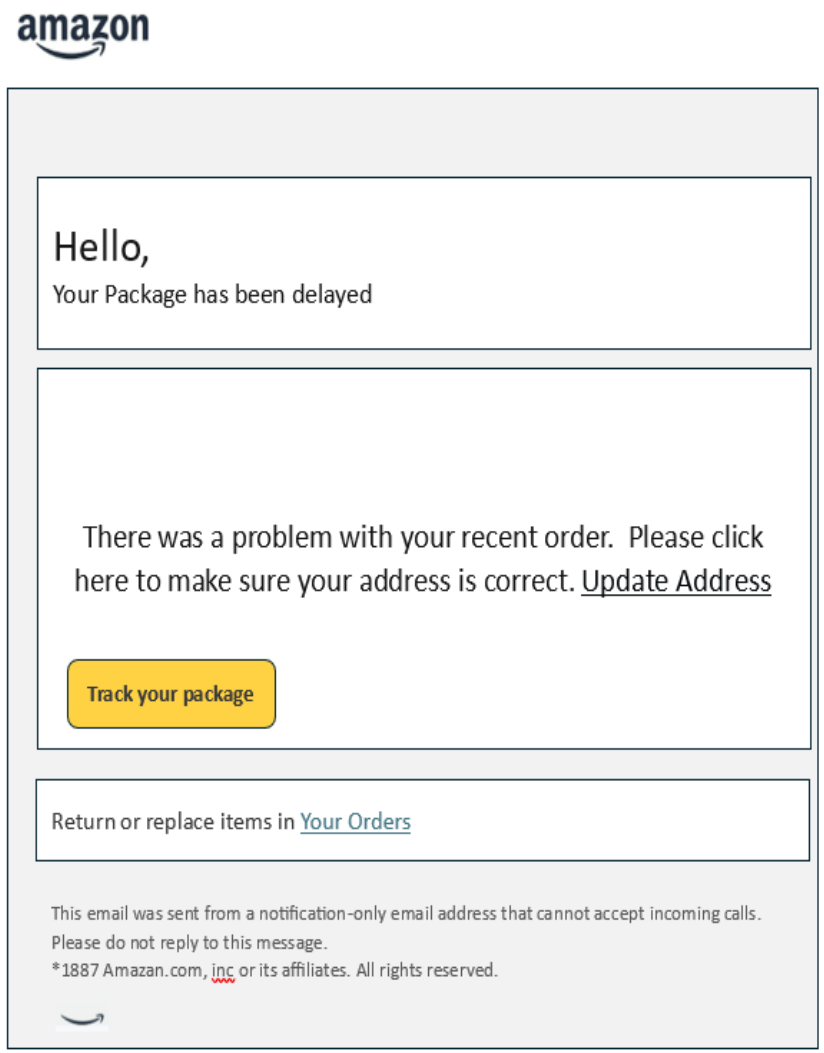
Can you spot the Phishing in this example?

To accounts@amazan.com

Cc

Subject URGENT-your Amazan.com order #113-4344446643 has been delayed, we need your assistance

Amazan.com order-delivery@amazan.com
to me



To accounts@amazan.com

Cc

Subject URGENT-your Amazan.com order #113-4344446643 has been delayed, we need your assistance

Amazan.com order-delivery@amazan.com
to me

Phishing Email

amazon

Hello,
Your Package has been delayed

There was a problem with your recent order. Please click here to make sure your address is correct. Update Address

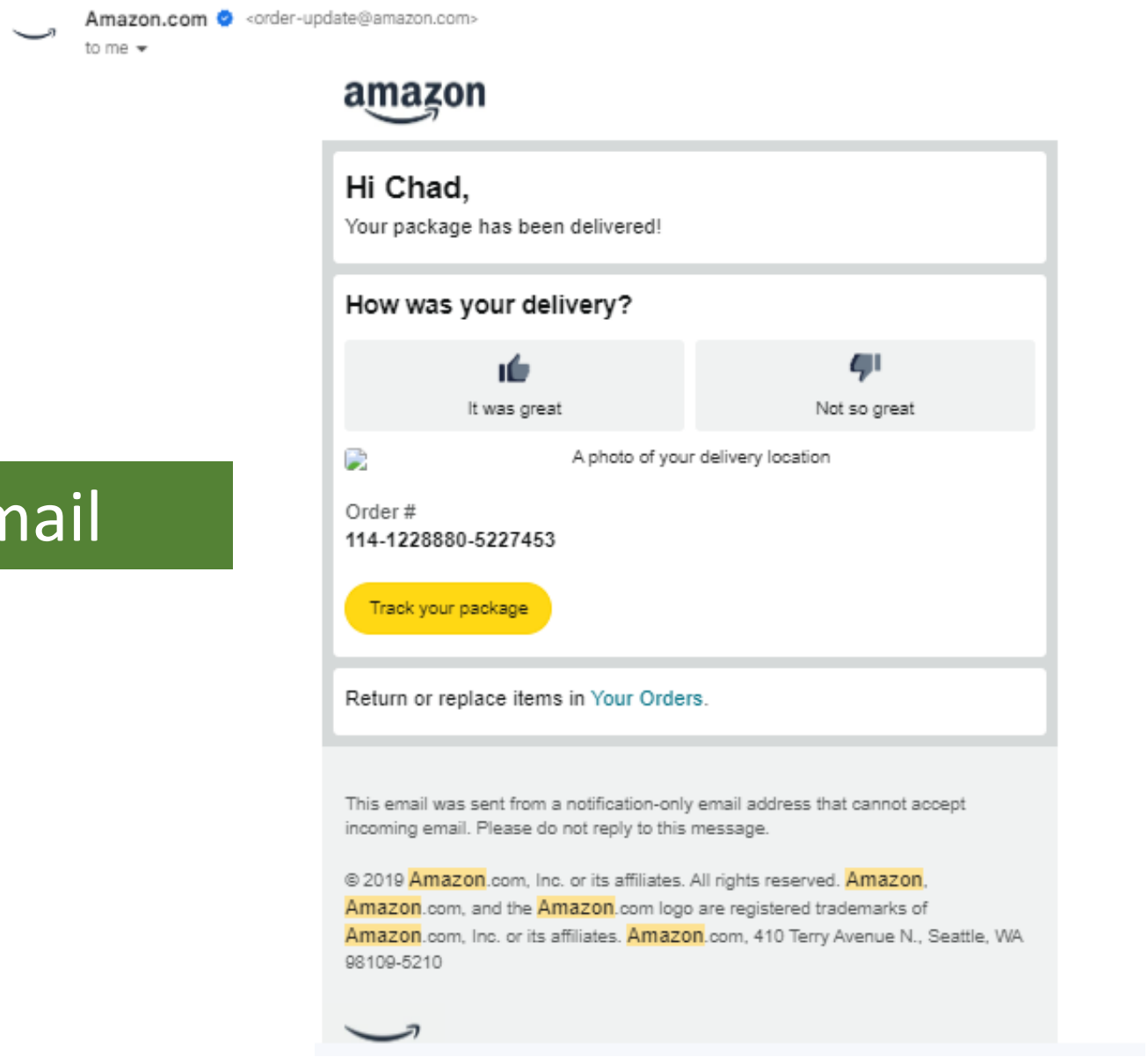
Track your package

Return or replace items in Your Orders

This email was sent from a notification-only email address that cannot accept incoming calls.
Please do not reply to this message.
*1887 Amazan.com, inc or its affiliates. All rights reserved.

How many flags did you see?

Safe Email



Amazon.com <order-update@amazon.com>
to me

amazon

Hi Chad,
Your package has been delivered!

How was your delivery?

It was great

Not so great

A photo of your delivery location

Order #
114-1228880-5227453

Track your package

Return or replace items in Your Orders.

This email was sent from a notification-only email address that cannot accept incoming email. Please do not reply to this message.

© 2019 Amazon.com, Inc. or its affiliates. All rights reserved. Amazon, Amazon.com, and the Amazon.com logo are registered trademarks of Amazon.com, Inc. or its affiliates. Amazon.com, 410 Terry Avenue N., Seattle, WA 98109-5210

From: email address: John@getmymoney.com

Subject: URGENT Transfer of Funds Required

Hello Dianne,

Please could you urgently transfer the funds enclosed in the attached invoice before you leave today.

Sorry to ask for this so close to the end of the day, the partner we are working with needs to receive the funds today or our project will fall through.

I would appreciate it if you could confirm when this has been completed.

Many thanks,

Rev. Issac

INSURANCE BOARD
Partners in Protection

Use Strong Passwords

CREATE STRONG PASSWORDS:

- **Long**
  - At least 16 characters
- **Unique**
  - NEVER reuse passwords
- **Complex**
  - Upper- and lower-case letters
  - Numbers
  - Special characters
  - Spaces

INSURANCE BOARD
Partners in Protection

Use a Password Manager

WHY USE A PASSWORD MANAGER?

- Stores your passwords
- Alerts you of duplicate passwords
- Generates strong new passwords
- Some automatically fill your login credentials into website to make sign-in easy

Encryption ensures that password managers never "know" what your passwords are, keeping them safe from cyber attacks.

Turn on Multifactor Authentication

WHAT IS IT?

- A code sent to your phone or email
- An authenticator app
- A security key
- Biometrics
  - Fingerprint
  - Facial recognition

Turn on Multifactor Authentication

WHERE SHOULD YOU USE MFA?

- Email
- Accounts with financial information
  Ex: Online store
- Accounts with personal information
  Ex: Social media

INSURANCE BOARD
Partners in Protection

Record/Data Retention Policy

- Written document retention policy ensures staff and volunteers follow consistent guidance retention and destruction- Sample

- Based on what type of documents must be retained and for how long. Research your state to see what you need to retain and for how long.

- Here is a list of records you should keep perinatally.
  - Articles of Incorporation
  - Audit reports, from independent audits
  - Corporate resolutions
  - Checks
  - Determination letter from the IRS, and any correspondence
  - Financial statements (year-end)
  - Insurance Policies
  - Minutes of board meetings and annual meetings of members
  - Tax returns
  - Real estate deeds, mortgages, bills of sale

INSURANCE BOARD
Partners in Protection

Incident Reporting

Why When Who

Incident Reporting

Why report cyber incidents?

- For situational awareness
- For decision making
- Requesting response assistance

When to report a cyber incident?

If there is a suspected or confirmed cyber attack or incident that:

- Affects core or critical business functions;
- Results in the loss of data, system confidentiality, integrity, and/ or availability; or control of systems;
- Indicates malicious software is present on critical systems

INSURANCE BOARD
Partners in Protection

Incident Reporting

Who to report cyber incidents to?

- Leadership, public affairs, legal and other internal stakeholders
- Relevant vendors
- Law enforcement and other government agencies
- Cyber insurance providers
- Appropriate 3rd party incident response teams

CISA
Report | CISA
report@cisa.gov
(888) 282-0870

FBI
Internet Crime Complaint Center (IC3)
www.ic3.gov

INSURANCE BOARD
Partners in Protection

Defend and Mitigate Cyber Risks

SECURE OUR WORLD

Teach Employees to Avoid Phishing

Require Strong Passwords

Require Multifactor Authentication

Update Business Software

Secure Our World | CISA

Building a Strong Cybersecurity Culture

- **Use basic cybersecurity training.** This helps familiarize staff with cybersecurity concepts and activities associated with implementing cybersecurity best practices.
- **Identify available cybersecurity training resources.** Cybersecurity training resources—on topics like phishing and good email practices—are available through professional association, educational institutions, as well as private sector and government sources.
- **Stay current on cybersecurity events and incidents.** This helps identify lessons learned and helps to maintain vigilance and agility to cybersecurity trends.
- **Encourage employees to make good choices online** and **learn about risks** like phishing and business email compromise.

INSURANCE BOARD
Partners in Protection

Cybersecurity Services

Conducted by CISA

Our insurance serves you so you can serve God.

ServeGod

No-Cost Cybersecurity Services and Tools

- In addition to following the mitigations, utilize CISA's Free Cybersecurity Services and Tools, which can be accessed by visiting https://www.cisa.gov/free-cybersecurity-services-and-tools.

INSURANCE BOARD
Partners in Protection

Cybersecurity Resources

- Partnership Development
  - Outreach Activities
  - Informational Exchanges (individual, group, etc.)
  - Committees and Working Groups support
  - Symposiums/ Conferences/ Webinars/ Cyber Camps
  - FBI Cyber Task Force Memberships

- Stakeholder Preparedness
  - Cybersecurity Workshops
  - Technical Exchange
  - Introductory Visits and Cyber Protective Visits (CPVs)
  - Cyber Exercises support/ *Tabletop Exercises*
  - Awareness and Cyber Threat Training/ Briefings

- Assessments
  - Cybersecurity Performance Goals assessments (CPGs)
  - Ransomware Readiness Assessments (RRAs)
  - Cyber Resilience Reviews (CRRs)
  - External Dependency Management Assessments (EDMs)

- Vulnerability Scanning
  - Cyber Hygiene Service (Public Attack Surface)
    - Known Exploitable Vulnerabilities (KEV)
  - Web Application Scanning
  - Penetration Testing

CISA No-Cost Cybersecurity Tools

- Assess Vulnerabilities:
  - Downloading and Installing CSET | CISA
  - Known Exploited Vulnerabilities Catalog | CISA
- Hardening:
  - CIS Benchmarks (cisecurity.org)
  - GitHub - decalage2/awesome-security-hardening: A collection of awesome security hardening guides, tools and other resources
  - Secure Cloud Business Applications (SCuBA) Project | CISA
    - GitHub - cisagov/ScubaGear: Automation to assess the state of your M365 tenant against CISA's baselines
    - https://www.cisa.gov/sites/default/files/publications/SCuBA_TRA_RFC_EG_508c.pdf

CISA No-Cost Cybersecurity Tools

Cyber Defense:

- Helping Cyber Defenders “Decide” to Use MITRE ATT&CK | CISA
- Logging Made Easy SIEM Tool
- CISA Releases RedEye: Red Team Campaign Visualization and Reporting Tool | CISA
- CISA Red Team Shares Key Findings to Improve Monitoring and Hardening of Networks | CISA
- Subscribe to Updates from CISA | CISA

INSURANCE BOARD
Partners in Protection

Insurance Perspective

• Cyber Insurance

Focuses on digital assets and risks associated with technology and the internet.

Cyber insurance covers intangible losses, such as data breaches, cyber extortion, business interruption, legal expenses, and public relations efforts.

It can also cover the costs of credit card fraud, identity theft, stolen funds, data loss and restoration, computer system repair, and damaged brand reputation

• Crime Insurance

Focuses on physical and financial assets and risks related to theft, fraud, and dishonesty.

Crime insurance covers tangible losses, such as money or merchandise theft, and securities.

It also covers losses that are not covered by other types of insurance policies, such as property insurance or liability insurance.

Our insurance serves you so you can serve God.

ServeGod

INSURANCE BOARD
Partners in Protection

Questions

Our insurance serves you so you can serve God.

ServeGod

INSURANCE BOARD
Partners in Protection

Resources

Non-Profit Risk.org data privacy and cyber liability article
https://nonprofitrisk.org/resources/articles/data-privacy-and-cyber-liability-what-you-dont-know-puts-your-mission-at-risk/
https://nonprofitrisk.org/login/

12 Security Control for insured by Marsh McLennan Agency

CISA.gov

IC3.org

Safety Central

Incident Response Guideline for Cyber Crimes

INSURANCE BOARD
Partners in Protection

YOUR Insurance Board Loss Control Team

Chad Cunningham, Director of Loss Control
ccunningham@insuranceboard.org

Monroe Moore, Loss Control Analyst
mmoore@insuranceboard.org