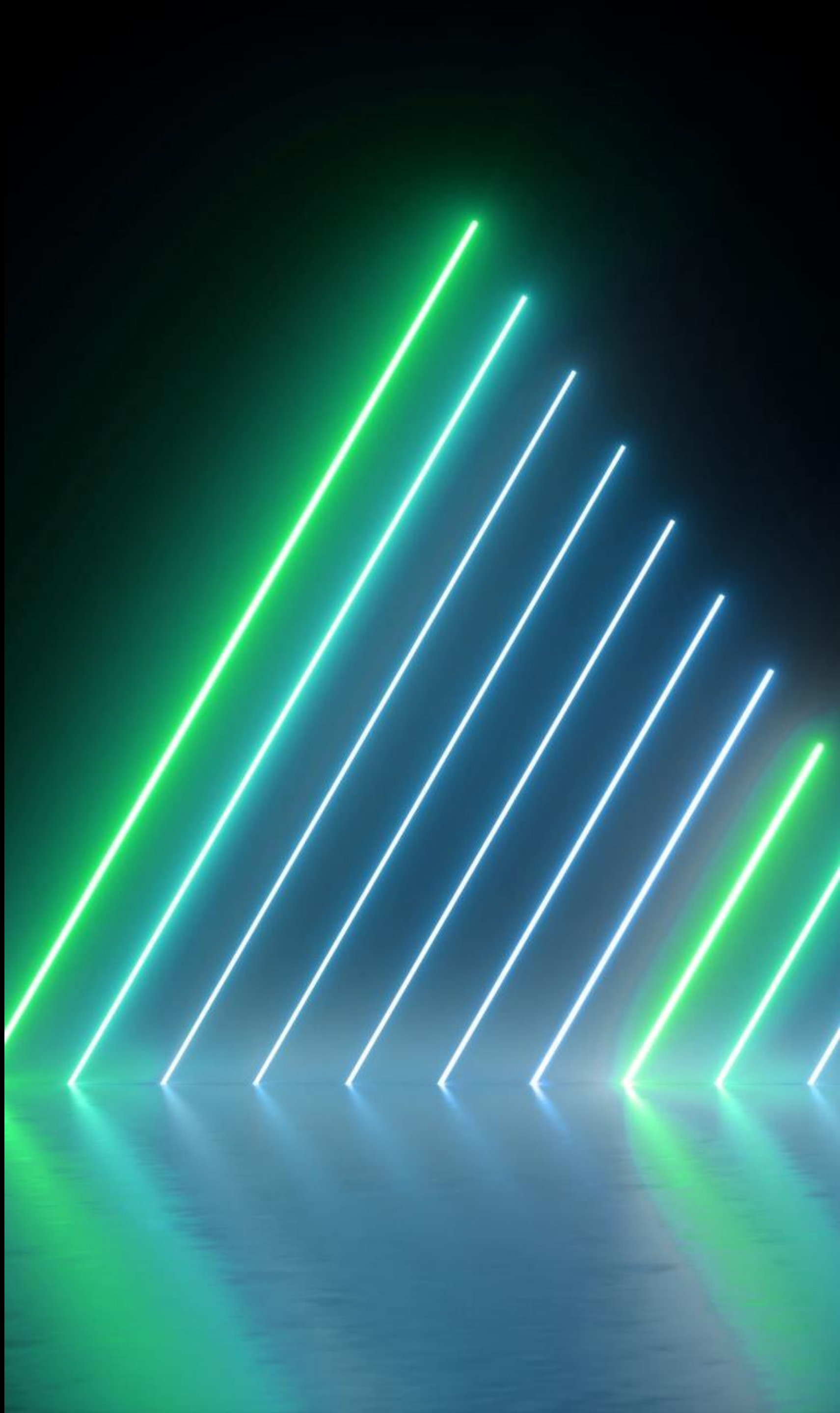
INFORMATION TECHNOLOGY SECURITY: BEST PRACTICE INTRODUCTION TRAINING WITH ABCNS, LLC.

Your one stop shop for all things technology related



COURSE OVERVIEW

I. ABCNS Introduction

II. Security Best Practice101

III. Conclusion

COURSE OBJECTIVES

By the end of this training session, you should be able to:

- Contact ABCNS through the proper channels to receive the best support for your technology needs
- Understand best cybersecurity practices to minimize risk

ABCNS, LLC.

YOUR TRUSTED SOURCE IN IT SERVICES & SUPPORT

ABCNS, LLC. was established in 2012 to provide IT Professional Services, SaaS, and On-Premises business applications and solutions that give clients/partners the ability to stay current in this ever-demanding and changing information technology. We strive to meet your business needs at all levels so you can focus on running your business.

The company was formed by Mr. Brian K. Bouchard and is a Massachusetts LLC company.

ABCNS, LLC

ABCNS, LLC. INTRODUCTION

Our Mission

Building on our technologies and competencies creating value for our customers. We’ll achieve this by focusing on the intersection of our client’s emerging needs and the acceleration of business and technological change

Our Values

Our values are the guiding principles upon which ABCNS was founded and how we strive to conduct our business on a daily basis. Values establish our view of the world as we shape the future. They determine how we treat each other

Our Approach & Culture

Our drive for exceptional service delivery is built on the belief that we are nothing if you are not satisfied with us. Our passion for helping you achieve your goals, no matter what, is what truly differentiates us from our competitors.

HOW TO GET SUPPORT FAST

EMAIL	CALL	CLIENT PORTAL
support@abcns.com	(617) 930-1300	https://www.abcns.com/clients

INTRODUCTION

- Cyber threats are evolving rapidly
- Data breaches result in financial loss, reputational harm, and personal consequences.
- Security awareness is key to protecting personal and corporate assets

CYBERSECURITY 101

- ⚠ Cybersecurity Quick Facts
- ☠ Social Engineering and its Types
- Symptoms of a Virus Infection
- 🔒 How you can mitigate risks

CYBERSECURITY QUICK FACTS

- Global Cybercrime Costs – Cybercrime is expected to cost the world $10.5 trillion annually by 2025, making it more profitable than the global drug trade.
- Ransomware Attacks – Ransomware remains one of the biggest threats, with a new attack occurring every 11 seconds.
- Data Breaches – In 2023, the average cost of a data breach reached $4.45 million, and it's expected to increase in 2024.
- Phishing Trends – Over 90% of cyberattacks start with phishing, and AI-powered phishing scams are becoming more sophisticated.
- Cloud Security Risks – With 80% of companies using cloud-based services, misconfigured settings are a major risk, accounting for nearly 70% of security incidents.
- Zero Trust Adoption – More businesses are adopting Zero Trust Security, meaning no user or device is automatically trusted, reducing attack surfaces.
- AI in Cybersecurity – AI is being used for both defensive and offensive cyber operations, increasing the complexity of security threats.
- IoT Vulnerabilities – By 2025, there will be over 75 billion IoT devices, making them a growing target for cybercriminals.
- Social Engineering – Attackers exploit human psychology rather than technical vulnerabilities, with deepfake scams rising.
- Nation-State Attacks – Geopolitical tensions have led to an increase in state-sponsored cyberattacks targeting critical infrastructure.

SOCIAL ENGINEERING ATTACKS

What is a Social Engineering attack?

Social engineering attacks manipulate people into:

- Sharing information that should not be shared
- Downloading software that they should not download
- Visiting websites they should not visit
- Sending money to unknown and unverified sources
- Making mistakes that compromise their personal or organizational security.

TYPES OF SOCIAL ENGINEERING ATTACKS

- Phishing
- Clone Phishing
- Pretexting
- Baiting
- Quid Pro Quo
- BEC (Business Email Compromise)
- Deepfaking
- Tailgating
- Spear Phishing & Whaling
- Smishing & Vishing
- Watering Hole Attacks
- Scareware
- Ransomware

SYMPTOMS OF A VIRUS INFECTION

1. Slow computer performance
2. Endless pop-ups and spam
3. Locked out of your computer
4. Changes to your homepage
5. Unknown programs starting on your computer
6. Mass emails sent from your email account
7. Security software disabled
8. Battery drains quickly
9. Frequent Crashes

HOW YOU CAN MITIGATE RISKS

- Physical Security
- Clean desk policy
- Strong Passwords
- Multifactor Authentication (2FA)
- Antivirus & Ransomware Protection
- Data Destruction
- Stay Alert & Educated
- Awareness & Timely reporting

- Think before you click
- Keep your system updated
- Back up your data
- Be wary of scams & phishing Attacks
- Secure your Wi-Fi
- Log out & Lock your Devices

PHYSICAL SECURITY

- Always lock your workstation when stepping away.
- Clean desk policy: keep sensitive documents in secure storage to prevent unauthorized access or exposure.
- Use security badges and access controls for restricted areas. Do not allow tailgating (allowing unauthorized individuals to follow into a restricted area), even if it appears impolite.
- Do not plug in unknown USB drives or devices.

PASSWORD SECURITY

- Use strong, unique passwords with at least 8 -12 characters.
- Avoid common words, birthdays, or sequential numbers.
- Implement Multi-Factor Authentication (MFA) for extra security.
- Use a password manager to securely store credentials.

DEVICE SECURITY

- Keep your operating system and software up to date.
- Enable automatic updates and patches.
- Use endpoint security tools such as firewalls and antivirus software.
- Lock your device when not in use.

EMAIL SECURITY

- Beware of phishing emails that mimic trusted sources.
- Never click on suspicious links or attachments.
- Always verify sender details before responding.
- Use spam filters to reduce unwanted emails.

SAFE BROWSING PRACTICES

- Think before you click!
- Only visit trusted websites with https encryption.
- Be cautious of pop-ups and ads that may contain malware.
- Avoid using public Wi-Fi without a VPN.
- Do NOT download files from unknown sources.

SECURE DATA HANDLING

- Encrypt sensitive files before sending or storing.
- Follow company policies for secure data storage.
- Do NOT share confidential information via unsecured platforms.
- Regularly back up important data.

INCIDENT REPORTING

- Immediately report any suspicious activity or breaches.
- Follow company protocols for incident handling.
- Do not attempt to fix security breaches without proper guidance.
- Participate in regular security awareness training.

CONCLUSION

- Cybersecurity is everyone’s responsibility.
- Stay alert and follow best practices to protect yourself and your organization.
- Keep learning and adapting to new security threats.
- Report any security concerns to the appropriate teams.
- Questions? Reach out to use at support@abcns.com