

CYBER SECURITY AWARENESS TRAINING DECK

WHAT IS CYBERSECURITY AND WHY IS IT SO IMPORTANT?

Cybersecurity is **the protection of systems, networks and data against malicious threats**. It's about preventing unauthorized access, theft or damage to these critical assets.

ESSENTIAL

- Wherever technology exists, cybersecurity safeguards it.

CRITICAL

- Protects personal, financial and sensitive information.
- Prevents costly breaches and operational downtime.
- Maintains compliance with regulations (e.g., GDPR, HIPAA).

APPLIES TO EVERYONE AND EVERYWHERE:

- Important for individuals, SMBs, enterprises and government entities.



**CYBER
SECURITY**
AWARENESS MONTH



REQUIRES A STRATEGIC APPROACH:

Tailoring security policies according to the organization's needs.

Integrating prevention, detection, response and recovery for a proactive approach.

Protecting operations to ensure business continuity.

OUTCOME:

A resilient posture that adapts to evolving threats.

**CYBER
SECURITY**
AWARENESS MONTH

FOUR EASY WAYS TO STAY SAFE ONLINE



USE A STRONG PASSWORD AND A PASSWORD MANAGER

LONG

At least 16 characters

UNIQUE

Never reuse passwords

RANDOM

Upper- and lower-case letters, numbers, special characters, spaces and consider using passphrases

FOUR EASY WAYS TO STAY SAFE ONLINE

PASSWORD MANAGER

- They act like a **safe for storing your passwords.**
- Alerts you to **duplicate passwords.**
- Generates **new, strong passwords.**
- Can **automatically fill in login credentials** on websites, making sign-in easier.
- **It won't fall for a phishing website**, even if you do!

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

TURNING ON MULTI-FACTOR AUTHENTICATION

- Email
- **Accounts with financial information**
(e.g., Online stores or banking)
- **Accounts with personal information**
(e.g., social media)



FOUR EASY WAYS TO STAY SAFE ONLINE

3

RECOGNIZE AND REPORT PHISHING ATTACKS

KEY SIGNS OF PHISHING:

- **A tone that's urgent or evokes fear.**
Example: "Click this link immediately or your account will be closed."
- **Sender's email address doesn't match the company sending it.**
Example: Amazon.com vs. Amaz0n.com
- **Unexpected communication.**
- **Requests to send personal info.**
Legitimate organizations don't ask for personal information through email or unexpected phone calls.
- **Misspelled words, bad grammar and strange URLs.**

**CYBER
SECURITY**
AWARENESS MONTH



FOUR EASY WAYS TO STAY SAFE ONLINE

4

UPDATE SOFTWARES

- **Updating devices and apps** ensures protection from the latest threats.
- **Clicking "Remind me later"** leaves you vulnerable to cyberthreats.
- **Automatic updates** are the easiest way to stay secure.
- These updates include phones, any portable device and computers.

**CYBER
SECURITY**
AWARENESS MONTH

CONTACT US.

Your complete cybersecurity partner

As your trusted MSP, we're here to protect your business from every angle — including backups, disaster recovery, endpoint protection, threat monitoring and compliance-ready security solutions. Whether you need proactive defense, rapid incident response or ongoing monitoring, we deliver full-spectrum cybersecurity services tailored to your business.

Boost your first line of defense — our Security Awareness Training helps your team recognize and stop phishing, ransomware and social engineering attacks before they cause harm.

Call us: +16012071047

Email: joel@catontech.com

Visit: