PHASE CONSULTING PRESENTS

Cybersecurity Awareness

JoAnne Green
Learning Innovation and Strategic Operations Manager

PU
PHASE UNIVERSITY

cyber awareness

[knowledge combined with attitudes and behaviors that serve to protect **personal** or **organizational information assets**. Being cyber aware means you understand **what the threats are**, and you take the right steps to prevent them.]

cyber literacy

[the ability to use **computer technologies** effectively and to simultaneously understand the **implications of those actions**. It is also important to know where to go to find reliable and accurate resources in cyberspace, otherwise known as cyber intelligence.]

cyber training

[cybersecurity technical skill development]

Before we begin

HOW "CYBERAWARE" ARE YOU?

When was the last time you changed your password on your email, mobile apps, banking, and online shopping websites?

Do you know how many emailing lists you're on and websites you have accounts for?

Are you aware of your surroundings and pay attention to people looking over your shoulder or eavesdropping while you're interacting online?

WHAT WE'LL LEARN
COURSE AGENDA

CYBER DOMAIN LANDSCAPE

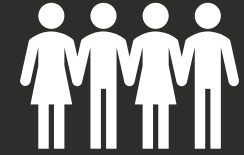Understand the language of cybersecurity and why awareness is a critical skill for the workplace.

THREATS & VULNERABILITIES

Overview of technical, environmental, and behavioral threats.

THREAT ACTORS

Identify individuals and organizations responsible for the majority of criminal activity.

VICTIMS

Understand what individuals, organizations, and technologies are most at risk and the impact of a cybersecurity incident.

WHAT WE'LL LEARN
COURSE AGENDA

PREVENTION & RESPONSE

Understand how to protect against cyber crime and how to respond if you are a target.

INDUSTRY DIFFERENCES

Overview of threats that are specific to different industry sectors.

THE LAW

Determine what laws and jurisdictions are involved in deterring and combatting cyber crime.

COMMITTMENT TO CHANGE

Development of a lifelong commitment to cyber education.

Companies spend millions of dollars on firewalls and secure access devices, and it's money wasted because none of these measures address the weakest link in the security chain: the people who use, administer and operate computer systems

— Kevin Mitnick —

PEOPLE CAN BE THE WEAKEST LINK OR THE STRONGEST SECURITY ASSET

THE PHASE UNIVERSITY TEAM