Cybersecurity Practices for Everyday Employees

OUTPUT WORKSHOP

✉ hello@output.training
☎ (844) 3OUTPUT

Course Description

This course teaches staff the practical habits that prevent the most common breaches: strong sign-in practices, spotting and reporting phishing, keeping devices and software up to date, using secure networks and file-sharing, and protecting data with backups and recovery plans. The focus is on simple, repeatable actions employees can apply immediately to reduce risk across email, web, and mobile. Good cyber hygiene improves security posture, reduces downtime, and limits financial and reputational damage when incidents occur.

Learning Tracks

Digital Transformation	Cybersecurity	Business Operations
Compliance	Remote Work	General

Why This Course Matters

- Most incidents start with everyday mistakes, correcting these habits delivers outsized risk reduction.
- Clear, job-relevant practices help non-technical staff share responsibility for security and keep sensitive data safe.
- A shared reporting culture shortens incident response time and limits impact when something does go wrong.

Who Should Attend

Relevant for all staff

Register Now

COURSE SYLLABUS

Course Overview

Build everyday security habits that protect company accounts, devices, and data.

What You'll Learn

1. Requirements discovery and caller journey mapping
2. AI and automation layers
3. Advanced call routing & IVR strategies
4. Queue and ring-strategy design
5. Visual flow documentation

Syllabus

1. Strong Passwords & Passphrases
2. Multi-Factor Authentication (MFA) Essentials
3. Phishing & Social Engineering
4. Safe Browsing & Links
5. Email Hygiene Basics
6. Device & Software Hygiene
7. Data Handling & File Sharing
8. Access & Permissions
9. Backups & Account Recovery
10. Reporting & Response Basics

Register Now

Check out our other courses at:

https://Output.Training