

# Corso di Avvicinamento al Digitale per il Personale ATA

## Sessione II

Benvenuti al corso! Imparerete a utilizzare strumenti digitali in modo sicuro e produttivo. Acquisire competenze informatiche è fondamentale per svolgere al meglio il vostro lavoro.

 **by Cresciscola** <sup>TM</sup>



# Importanza della Sicurezza Informatica

Protezione dei Dati	I dati sensibili devono essere protetti da accessi non autorizzati
Rispetto della Privacy	I requisiti di privacy come il GDPR devono essere rispettati
Mantenere la Fiducia	La sicurezza favorisce la fiducia delle famiglie e degli studenti
Evitare Problemi Legali	Violazioni possono causare sanzioni e danni di immagine



# Cenni di GDPR e Protezione Dati

## 1 Privacy dei Dati

Il GDPR stabilisce norme sulla raccolta e l'uso dei dati personali.

## 2 Sicurezza

È fondamentale proteggere i dati da accessi non autorizzati.

## 3 Consenso

I dati personali devono essere trattati solo con il consenso dell'interessato.

# Privacy delle Informazioni Personali

## Limitare la Condivisione

Condividere informazioni personali solo quando strettamente necessario.



## Attenzione sui Social Media

Impostare correttamente le opzioni di privacy sui social.



## Gestire i Cookie

Limitare i cookie di tracciamento per proteggere la privacy online.



# Configurazione Impostazioni di Privacy

1

## Google Drive

Configurate le impostazioni di condivisione e visibilità dei file.

2

## Gmail

Regolate le preferenze di privacy per la posta elettronica.

3

## Google Calendar

Controllate le autorizzazioni degli eventi condivisi.



# Utilizzo Sicuro di Internet

## 1 Siti Web Affidabili

Navigare solo su siti web verificati e sicuri.

## 2 Aggiornamenti Software

Mantenere aggiornati sistemi operativi e applicazioni.

## 3 Password Complesse

Utilizzare password sicure e uniche per ogni account.

## 4 Connessioni Crittografate

Assicurarsi che le connessioni siano crittografate (HTTPS).

# Condivisione Sicura dei Documenti



## Restrizioni

Applicate limitazioni di accesso ai file sensibili.



## Condivisione Sicura

Condividete file solo con destinatari autorizzati.



## Gestione Permessi

Assegnate autorizzazioni di modifica o sola visualizzazione.

# Esercizio: Privacy su Google Drive

1

## **Accedere a Drive**

Aprire Google Drive dal vostro account.

2

## **Selezionare un File**

Scegliete un documento da configurare.

3

## **Modifica le Impostazioni**

Cambiate le opzioni di condivisione e visibilità.

4

## **Salvataggio**

Salvate le modifiche per completare l'esercizio.

# Esercizio: Impostazione di Autorizzazioni

1

## **Creare un Documento**

Aprire un nuovo documento di testo.

2

## **Condividere**

Aggiungete collaboratori ed editori.

3

## **Assegnare Ruoli**

Impostate le autorizzazioni per ogni utente.

4

## **Testare le Autorizzazioni**

Verificate che le impostazioni funzionino correttamente.

# Riconoscimento delle Minacce Online

## **Malware**

Virus, worm e trojan che infettano i dispositivi.

## **Phishing**

Tentativi di rubare informazioni tramite email fraudolente.

## **Furto di Identità**

Appropriazione illecita di dati personali per scopi illeciti.

## **Attacchi di Rete**

Intrusioni non autorizzate nei sistemi di rete.

# Riconoscimento di Email di Phishing

## Mittente Sconosciuto

Fate attenzione a indirizzi email non verificati.



## Linguaggio Allarmistico

Evitate messaggi che creano un senso di urgenza.



## Link Sospetti

Non cliccate su link da fonti non affidabili.



# Esercizio: Simulazione di Attacco Phishing

## Preparazione

Studiate alcuni esempi di email di phishing.

1

## Simulazione

Riceverete email fittizie per rilevare potenziali minacce.

2

## Analisi

Discuterete insieme le caratteristiche delle email simulate.

3



# Strategie di Protezione

## Antivirus

Utilizzare software antivirus aggiornati per rilevare e rimuovere malware.



## Firewall

Configurare un firewall per filtrare il traffico di rete pericoloso.



## Formazione

Formare il personale sulle migliori pratiche di sicurezza online.



# Tecniche di Backup e Ripristino Dati

## **Backup Regolari**

Programmate backup periodici dei vostri dati.

## **Archiviazione Sicura**

Utilizzate supporti di archiviazione affidabili e crittografati.

## **Verifica Backup**

Testate regolarmente i backup per assicurarne l'integrità.

## **Piani di Ripristino**

Preparate procedure per recuperare rapidamente i dati.

# Riepilogo dei Concetti Chiave



## Protezione dei Dati

Mantenere i dati al sicuro da accessi non autorizzati.



## Configurazione Privacy

Regolare le impostazioni per controllare la condivisione.



## Sicurezza delle Email

Riconoscere potenziali minacce di phishing.



## Collaborazione Sicura

Gestire autorizzazioni e gruppi di lavoro.

# Esercizio: Verifica delle Impostazioni di Privacy

## Account di Posta

Controllate le impostazioni di privacy della vostra email.

1

2

## Social Network

Esaminare i profili sui social e le autorizzazioni di condivisione.

3

## Navigazione Web

Verificate le estensioni del browser e le impostazioni dei cookie.

4

## Dispositivi Mobili

Controllate le autorizzazioni delle app sui vostri dispositivi.