



Iniziativa realizzata da:



**SERVIZI BANCARI E ASSICURATIVI**

in collaborazione con:



# CORSO DI CYBER SECURITY

**Sicurezza  
informatica:  
più competenza e  
consapevolezza per  
contrastare furti di  
dati e truffe.**

**28 SETTEMBRE 2023 ORE 17:30**  
Museo Civico di Palazzo Elti  
Via Giuseppe Bini 9 - Gemona

**INIZIATIVA DEDICATA A SOCI E  
CLIENTI DI PRIMACASSA**

- Massimo 30 partecipanti

**Priorità di iscrizione  
dedicata ai Soci di PrimaCassa**

## PROGRAMMA

- **17:30**  
visita guidata del Duomo di Gemona

- **18:30**  
corso formativo  
sulla Cyber Security

- **19:30** saluti



## PROGRAMMA DEL CORSO

### CYBER SECURITY:

- Gli attori
- I Malware: le armi degli attacker

### CONOSCERE IL RISCHIO:

- Tipologie di rischio
- Gestione del rischio
- Trattamento del rischio

### LA SUPERFICIE D'ATTACCO

#### ATTACCHI INFORMATICI:

- Struttura degli attacchi informatici
- Social engineering (Baiting, Phishing, Whaling, Pretexting, Scareware)
- Malware via email (Trojan, Ransomware)
- Malware via USB e CD

#### DIFENDERSI DAGLI ATTACCHI INFORMATICI:

- Soluzioni di difesa adottate del reparto IT
- Difendersi dalle email malevole

#### PREVENIRE GLI ATTACCHI INFORMATICI:

- Gestione delle password
- MFA
- Ridurre la superficie di attacco

# MITI DA SFATARE E CONSIGLI PRATICI

## Prossimi corsi aperti a tutti:

9 eventi della durata di un'ora ciascuno con diversi punti di approfondimento in 9 diversi luoghi culturali del FVG.

Il corso di Cyber Security per Utenti Privati è orientato a tutti i cittadini che usino il PC e/o lo smartphone nella vita di tutti i giorni. I corsisti avranno modo di capire le dinamiche di base della sicurezza informatica domestica, imparando a riconoscere i vari tipi di attacchi mirati all'utente, e scoprendo quali strategie mettere in atto per evitare di essere vittima di detti attacchi.

## PROGRAMMA BASE COMUNE A TUTTI GLI EVENTI

### COS'È LA CYBER SECURITY

- Gli attori
- Gli obiettivi degli attacker
- I Malware: le armi degli attacker
- Il social engineering

### APPROFONDIMENTI DIVERSI PER OGNI EVENTO

#### 1. SOCIAL ENGINEERING: PHISHING/SMISHING/VISHING/BAITING

- Le tipologie di attacco via email
- Riconoscere un messaggio fraudolento

#### 2. ALLEGATI E DOWNLOAD MALEVOLI DELLE EMAIL

- Come riconoscere i file che possono rappresentare una minaccia

#### 3. LA NAVIGAZIONE SU INTERNET

- Attenzione ai domini
- Aggiornare il browser
- Prestare attenzione ai siti di eCommerce non convenzionali
- Usare sistemi di pagamento sicuri

#### 4. I RISCHI DELLE CHIAVETTE USB

- Perché le chiavette sono pericolose
- Come mitigare il rischio

#### 5. GESTIONE DELLE PASSWORD

- Come si valuta la complessità di una password

- Gli errori comuni
- I criteri per creare una password solida
- Archiviazione corretta delle password

#### 6. L'IMPORTANZA DELL'MFA

- Cos'è l'MFA
- Perché è importante
- Quali servizi già la prevedono (banca, SPID)

#### 7. PROTEGGERE IL PROPRIO PC

- Aggiornamenti
- Antivirus
- Buone prassi

#### 8. SICUREZZA NEI DISPOSITIVI MOBILI

- Perché è importante proteggere lo smartphone
- PIN, Password, e Biometria

#### 9. LA SICUREZZA SUI SOCIAL NETWORK

- I pericoli dell'eccessiva diffusione delle informazioni
- Usare le impostazioni di privacy