# Catalogo Corsi Exprivia

Ottobre 2024

# Esercitazioni di phishing

## Descrizione attività

Il servizio di Esercitazioni di Phishing offre, attraverso una combinazione di simulazioni realistiche e analisi dei risultati, un approccio completo e personalizzato per testare la capacità dei partecipanti a riconoscere e segnalare opportunamente un tentativo di Phishing.

## Modalità di svolgimento

L'esercitazione prevede l'invio di email di phishing simulato ai dipendenti dell'azienda e la registrazione delle loro reazioni. È articolata in due sessioni, che si svolgeranno prima e dopo la partecipazione degli utenti ai corsi di formazione specifici. La gestione di ciascuna sessione di phishing avviene tramite una piattaforma sviluppata da Exprivia, che consente di creare e gestire una campagna di phishing personalizzata, con la possibilità di variare i modelli di email all'interno della stessa campagna. Al termine della campagna, viene generato un report dettagliato con statistiche e informazioni sui risultati ottenuti.

## Obiettivo del training

L’obiettivo del training consiste nel valutare le capacità iniziali dei partecipanti (durante la prima sessione) e verificare i miglioramenti (durante la seconda sessione) in termini di consapevolezza acquisita a seguito della preparazione ottenuta con i corsi di formazione.

# Corso: Cybersecurity Fundamentals

**Titolo corso**
Cybersecurity Fundamentals

**Modalità di erogazione**
Sessione con docente da remoto oppure in presenza

**Motivazione del corso**
Il corso “Cybersecurity Fundamentals” fornisce una conoscenza di base utile a sviluppare un approccio consapevole al tema della sicurezza informatica con particolare focus sulle principali minacce informatiche, sui concetti di processo e controllo di sicurezza e sulle best practice più rilevanti

**Durata**
4 ore

**Destinatari**
Manager/Dirigenti/Dipendenti

## Contenuto del corso

Le principali tematiche trattate nel corso sono:

- Definizione di cyber attacco e incidente di sicurezza informatico;
- Analisi delle principali tecniche di attacco utilizzate nello spazio cyber;
- Presentazione delle fasi che compongono la Kill-chain tipica di un attacco di sicurezza;
- Definizione dei controlli e processi di sicurezza atti a contrastare gli attacchi di sicurezza;
- Approfondimento sulle  Organizzazioni responsabili, all'interno di un'azienda, di implementare i controlli e i processi di sicurezza.

## Obiettivo del corso

Il corso ha l’obiettivo di incrementare il livello di consapevolezza di cybersecurity dei partecipanti promuovendo:

- La comprensione del modello di attuazione di un attacco informatico (cyber Kill-chain) e delle principali tipologie di attacco;
- La conoscenza di nozioni e concetti fondamentali in ambito cybersecurity;
- Fornire gli strumenti per identificare rischi e contromisure.

# Corso: Introduzione a NIS2

**Titolo corso**
**Introduzione a NIS2**

**Modalità di erogazione**
**Sessione con docente da remoto oppure in presenza**

**Motivazione del corso**
**Il corso "Introduzione a NIS" esplora la Direttiva NIS2, in vigore dal 2024, che mira a garantire un livello più elevato di protezione dalle minacce digitali.**

**Durata**
**8 ore**

**Destinatari**
**Dirigenti, CIO, CISO, product manager, IT Manager**

## Contenuto del corso

- **Prima parte**: Introduzione alla direttiva NIS2 in senso più ampio, differenze con la direttiva precedente, principali obblighi, relazioni con altre normative, indicazioni, best practices e contestualizzati per il settore sanitario.
- **Seconda parte**: Analisi delle misure di sicurezza indicate dalla direttiva, aspetti tecnologici sull'implementazione dei controlli
    - Aspetti organizzativi e di cybersecurity governance per il mantenimento e miglioramento continuo, processi da implementare e iniziative da pianificare.

## Obiettivo del corso

L'obiettivo del corso è quello di fornire ai partecipanti gli strumenti adeguati per rapportarsi alla nuova normativa, pianificare e implementare le mitigazioni identificate.

# Corso: Cybersecurity Governance

**Titolo corso**
Cybersecurity Governance e Risk management

**Modalità di erogazione**
Sessione con docente da remoto oppure in presenza

**Motivazione del corso**
Attraverso la governance, consigli di amministrazione e dirigenti svolgono un ruolo fondamentale per creare un'organizzazione cyber-resiliente.

**Durata**
8 ore

**Destinatari**
Dirigenti, CIO, CISO, Compliance, Governance

## Contenuto del corso

- **Il percorso di ogni organizzazione verso la resilienza informatica è diverso.**
- **Questo corso fornisce una direzione generale di viaggio.**
  - Per affrontare le singole complessità della governance è necessario che i leader traccino il percorso specifico della propria organizzazione.
- **I termini resilienza informatica e sicurezza informatica sono entrambi approfonditi in questo corso.**
  - La resilienza informatica è suggerita come un obiettivo realistico per un'organizzazione.

## Obiettivo del corso

Il corso "Cybersecurity Governance e Risk management" esplora le tematiche del governo della Cybersecurity e perché questo è fondamentale per minimizzare i costi associati ad una corretta gestione della sicurezza di una organizzazione, pur massimizzando la riduzione del Rischio Cyber .

.

# Corso: Phishing and How To Avoid it

**Titolo corso**
**Phishing and How to avoid it**

**Modalità di erogazione**
**Sessione con docente da remoto oppure in presenza**

**Motivazione del corso**
**Il corso "Phishing and How to avoid it" è pensato per fornire una comprensione approfondita del fenomeno del Phishing con lo scopo di sensibilizzare i partecipanti ad adottare comportamenti consapevoli atti a limitare tale minaccia e di presentare strategie utili per rilevare e difendersi da questa minaccia.**

**Durata**
**1 ora**

**Destinatari**
**Dipendenti**

## Contenuto del corso

Il corso "Phishing and How to avoid it" si suddivide in sei sezioni:

- **Introduzione** - Presentazione dei contenuti del corso;
- **Social Engineering e Phishing** - Fornisce una descrizione dettagliata dei concetti di Social Engineering e di Phishing e presenta le varianti di Phishing più diffuse;
- **Conseguenze del Phishing** – Contiene una analisi delle principali e possibili conseguenze legate al successo di un attacco di Phishing;
- **Riconoscere una mail di Phishing** – Descrive gli accorgimenti da adottare per riconoscere una email di Phishing;
- **Difendersi dal Phishing** – Illustra gli strumenti e i comportamenti utili per difendersi da attacchi di Phishing;
- **Conclusioni** – Contiene considerazioni di fine corso.

## Obiettivo del corso

- Il corso ha l'obiettivo di fornire una conoscenza teorica del Phishing e gli strumenti di base per rilevare e difendersi da tale minaccia.

# Corso: Social Engineering

**Titolo corso**
Social Engineering

**Durata**
2 ore

**Modalità di erogazione**
Sessione con docente da remoto oppure in presenza

**Destinatari**
Dipendenti

**Motivazione del corso**
**Il corso "Social Engineering" esplora le strategie e le tecniche adoperate dagli aggressori per sfruttare la vulnerabilità umana al fine di avere accesso a sistemi o informazioni sensibili. Il corso affiancherà all'approfondimento teorico degli aspetti rilevanti della Social Engineering, l'analisi di alcuni casi reali.**

## Contenuto del corso

- **Introduzione** - Definizione di Social Engineering e analisi obiettivi e motivazioni degli aggressori;
- **Principali tecniche di Social Engineering** - Approfondimento sulle principali tecniche utilizzate dai cybercriminali (Phishing, Quishing, BEC, Baiting, Pretexting, ecc)
- **Come riconoscere e prevenire attacchi di Social Engineering** - Strategie per prevenire e mitigare gli attacchi di Social Engineering;
- **Casi reali di attacchi di Social Engineering** – Analisi di alcuni esempi di attacchi di Social Engineering.

## Obiettivo del corso

L'obiettivo del corso è quello di fornire ai partecipanti gli strumenti adeguati per:

- Comprendere le motivazioni e delle tecniche utilizzate dagli aggressori nella Social Engineering;
- Individuare i segnali di potenziali attacchi di Social Engineering;
- Comprendere e adottare comportamenti sicuri e per prevenire le trappole della Social Engineering.

# Corso: Analisi dei rischi per la Sicurezza del Sistema informativo: identificazione e gestione

**Titolo corso**
**Analisi dei rischi per la Sicurezza del Sistema informativo: identificazione e gestione**

**Durata**
**10 ore**

**Modalità di erogazione**
**Sessione con docente da remoto**
**Oppure in presenza**

**Destinatari**
**Dipendenti**

**Motivazione del corso**
**Il corso "Analisi dei rischi per la Sicurezza del Sistema informativo: identificazione e gestione" esplora i processi di valutazione e trattamento del rischio e fornisce strumenti, standard e framework per l'analisi e la gestione del rischio informatico.**

## Contenuto del corso

- **Introduzione –** Presentazione dei principali concetti in ambito Sicurezza delle informazioni;
- **Il Rischio informatico** - Definizione metodologia di calcolo del rischio informatico;
- **Cyber risk management** - Panoramico del processo di gestione del rischio informatico;
- **Standard e framework** - La gestione del rischio nei principali standard e framework di sicurezza informatica.

## Obiettivo del corso

L'obiettivo del corso è quello di fornire ai partecipanti gli strumenti adeguati per:

- Comprendere il contesto aziendale e stabilire l'ambito del rischio;
- Analisi e valutazione del rischio;
- Implementare trattamenti adeguati per mitigare i rischi.

# Corso: Data Protection

**Titolo corso**
Data Protection

**Modalità di erogazione**
Sessione con docente da remoto oppure in presenza

**Motivazione del corso**
Il corso "Data Protection" mira a presentare i concetti fondamentali relativi alla protezione dei dati personali e ad approfondire la struttura, lo scopo, i principi e gli obblighi previsti dal regolamento General Data Protection Regulation (GDPR).

**Durata**
5 ore

**Destinatari**
Dipendenti

## Contenuto del corso

- **Introduzione alla protezione dei dati** – Presentazione dei concetti fondamentali;
- **Cos'è il GDPR** – Principi ed ambiti di applicazione del regolamento GDPR;
- **Principali entità del GDPR** - Panoramica sulle entità presentate all'interno del regolamento, i loro diritti e obblighi;
- **Sicurezza del trattamento e relative misure di sicurezza** - descrizione delle misure tecniche e organizzative per garantire la sicurezza del trattamento

## Obiettivo del corso

L'obiettivo del corso è quello di fornire ai partecipanti gli strumenti adeguati per:

- Comprendere i concetti fondamentali legati alla protezione dei dati;
- Avere una visione chiara dello scopo, dei principi e degli obblighi previsti dal GDPR;
- Approfondire l'adozione di misure adeguate al fine di garantire la sicurezza dei dati.

# Corso: Cyber Threat Intelligence

**Titolo corso**
Cyber Threat Intelligence

**Modalità di erogazione**
Sessione con docente da remoto oppure in presenza

**Durata**
Variabile (in base al livello di dettaglio richiesto)

**Destinatari**
Dipendenti

**Motivazione del corso**
Il corso "Cyber Threat Intelligence" esplora i concetti fondamentali legati al contesto della Cyber Threat Intelligence fornendo un panoramica sulle modalità e gli strumenti con cui vengono raccolti, condivisi e analizzati i dati relativi alle minacce informatiche al fine di promuovere la creazione di una base di conoscenza utile nella prevenzione e nella risposta agli incidenti.

## Contenuto del corso

- **Introduzione** – Definizione, scopi e principali concetti relativi alla Cyber Threat Intelligence;
- **Fonti di informazione** - Approfondimento sulle principali fonti di informazioni utilizzate durante l'attività di Threat Intelligence;
- **Analisi delle minacce** - Panoramica sui principali metodologie di analisi delle minacce;
- **Casi studio** – Analisi di alcuni attacchi informatici reali.

## Obiettivo del corso

L'obiettivo del corso è quello di fornire ai partecipanti gli strumenti adeguati per:

- Comprendere i concetti fondamentali relativi alla Cyber Threat Intelligence;
- Conoscere le principali fonti di informazione utili nella fase di raccolta dati;
- Conoscere i principali modelli e metodologie di analisi delle minacce;

# Corso: Application Security

**Titolo corso**
Application Security

**Modalità di erogazione**
Sessione con docente da remoto oppure in presenza

**Durata**
30 ore (modulabile in base alle esigenze)

**Destinatari**
Tecnici

**Motivazione del corso**
Il corso "Application Security" è pensato per formare professionisti in grado di sviluppare software sicuro fin dalle prime fasi del ciclo di vita dello sviluppo. con le linee guida AgID e l'OWASP Top 10. Il corso fornisce le competenze necessarie per prevenire vulnerabilità comuni, ridurre il rischio di attacchi e migliorare la sicurezza del codice.

## Contenuto del corso

- Fondamenti di Application Security e il ciclo di vita dello sviluppo software sicuro.
- Introduzione al Security by Design e Security by Default: principi e best practices.
- Panoramica dettagliata dell'OWASP Top 10: vulnerabilità principali e come mitigarle.
- Analisi delle linee guida AgID per lo sviluppo di codice sicuro nelle pubbliche amministrazioni.
- Tecniche di coding sicuro: gestione dell'autenticazione, autorizzazione, gestione degli input.
- Strumenti e metodologie per la verifica della sicurezza nelle applicazioni: Analisi Statica e Analisi Dinamica.
- Esercitazioni pratiche su analisi e correzione delle vulnerabilità del codice con l'utilizzo di strumenti software.

## Obiettivo del corso

L'obiettivo del corso è quello di fornire ai partecipanti gli strumenti adeguati per:

- Comprendere i concetti chiave della sicurezza delle applicazioni e le sfide principali.
- Applicare i principi di Security by Design e Security by Default nello sviluppo del software.
- Conoscere e mitigare le vulnerabilità incluse nell'OWASP Top 10.
- Implementare pratiche di sviluppo sicuro seguendo le linee guida AgID.
- Utilizzare strumenti e tecniche per testare e verificare la sicurezza del codice.
- Ridurre il rischio di attacchi migliorando la sicurezza durante tutto il ciclo di vita dell'applicazione.

# Corso: Rilevamento e valutazione delle minacce

**Titolo corso**
**Rilevamento e valutazione delle minacce**

**Durata**
**20 ore / 40 ore (modulabile in base alle esigenze)**

**Modalità di erogazione**
**Sessione con docente da remoto oppure in presenza**

**Destinatari**
**Tecnici**

**Motivazione del corso**
**Il corso "Rilevamento e valutazione delle minacce" nasce dall'esigenza di formare professionisti in grado di identificare, analizzare e mitigare le vulnerabilità presenti in sistemi, applicazioni e reti. Il corso offre una panoramica sugli strumenti più utilizzati nel settore, fornendo competenze pratiche e teoriche per migliorare la resilienza aziendale.**

## Contenuto del corso

- Introduzione alla sicurezza informatica e alle vulnerabilità.
- Panoramica sulle attività di VAPT e WAPT: differenze, obiettivi e metodologie.
- Strumenti principali per il Vulnerability Assessment (scanner e tool di automazione).
- Tecniche e strumenti di Penetration Testing su reti e applicazioni web.
- Analisi dei risultati, generazione di report e proposte di mitigazione.
- Esercitazioni pratiche con casi reali e simulazioni.

## Obiettivo del corso

L'obiettivo del corso è quello di fornire ai partecipanti gli strumenti adeguati per:

- Comprendere le basi delle vulnerabilità e delle minacce informatiche.
- Distinguere tra Vulnerability Assessment, Penetration Testing (VAPT) e Web Application Penetration Testing (WAPT).
- Conoscere e saper utilizzare i principali strumenti di valutazione delle vulnerabilità.
- Eseguire test di sicurezza su reti e applicazioni web, identificando potenziali punti di attacco.
- Sviluppare report dettagliati su vulnerabilità e rischi, con proposte di mitigazione.
- Applicare le tecniche apprese in scenari reali attraverso esercitazioni pratiche.

# Corso: Cloud Security

**Titolo corso**
Cloud Security

**Modalità di erogazione**
Sessione con docente da remoto oppure in presenza

**Durata**
80 ore (modulabile in base alle esigenze)

**Destinatari**
Tecnici

**Motivazione del corso**
Il corso di Cloud Security si concentra sull'insegnamento delle competenze, delle conoscenze e delle tecniche necessarie per proteggere i dati e le risorse nel cloud, affrontando le principali sfide e minacce di sicurezza specifiche per le infrastrutture cloud. Il corso fornisce una panoramica dei principi fondamentali della sicurezza informatica e di come si applicano ai vari modelli di cloud computing

## Contenuto del corso

- **Introduzione al Cloud** - Introduzione alle tipologie del Cloud Computing;
- **Minacce nel Cloud** - Definizione dei rischi principali per le aziende che adottano infrastrutture cloud;
- **Controllo accessi a livello aziendale** - Processo attraverso cui un'organizzazione gestisce e regola chi può accedere a risorse e dati;
- **Accesso federato** - Gestione delle identità che consente agli utenti di accedere a servizi o sistemi con un'unica identità digitale;
- **La sicurezza nei tenant cloud -** Protezione dei dati e delle risorse di ogni cliente (tenant) in un ambiente cloud condiviso;
- **Identity access management (IAM) -** Sistema che gestisce le identità digitali e controlla l'accesso degli utenti alle risorse aziendali;
- **Logging e monitoring -** Registrazione degli eventi e dei controlli dei sistemi per la sicurezza del cloud;
- **Incident response -** Processo di gestione e risposta a eventi di sicurezza informatica che possono compromettere il cloud;
- **Sicurezza dei dati -** Pratiche e tecnologie utilizzate per proteggere le informazioni da accessi non autorizzati;
- **Gestione delle operazioni -** Pianificazione, esecuzione e supervisione delle attività necessarie per il miglioramento dei servizi cloud;
- **OAUTH2 + OpenID Connect -** Protocolli di autorizzazione e autenticazione utilizzati per gestire l'accesso alle risorse del cloud;
- **Progettazione sicura –** Progettazione che integra la sicurezza nella fase di disegno del software e sistemi.

## Obiettivo del corso

L'obbiettivo del corso è fornire le competenze e le conoscenze necessarie per garantire la sicurezza delle infrastrutture cloud, delle applicazioni e dei dati ospitati su piattaforme cloud, attraverso l'implementazione di misure preventive, correttive e di monitoraggio continuo. I partecipanti imparano a identificare, valutare e mitigare i rischi legati all'uso del cloud, comprendendo le principali vulnerabilità e minacce, e implementando strategie di sicurezza efficaci.

# Corso: Elementi di Crittografia

**Titolo corso**
Elementi di Crittografia

**Modalità di erogazione**
Sessione con docente da remoto oppure in presenza

**Motivazione del corso**
Il corso evidenzia come la Crittografia è fondamentale per garantire la riservatezza e l'integrità delle informazioni, ed è uno degli strumenti chiave per prevenire accessi non autorizzati e proteggere le infrastrutture digitali.
Le tecnologie crittografiche evolvono costantemente e la conoscenza di questi strumenti rappresenta un vantaggio competitivo per chi lavora in ambito IT, Cybersecurity o sviluppo Software.

**Durata**
50 ore (modulabile in base alle esigenze)

**Destinatari**
Tecnici

## Contenuto del corso

- **Introduzione -** Ruolo della crittografia come arma tattica nella strategia della Cyber Security.
- **Concetti crittografici generali** - Cosa è la crittografia, cenni storici.
- **Algoritmi Simmetrici** – Diffusione, Confusione, XOR, Cifrario a blocchi, principali Algoritmi, Esercitazioni con OpenSSL.
- **Algoritmi di Hashing** – Funzione Hash, Principali Algoritmi di Hash, Funzione Hash e Autenticazione Challenge Response, Esercitazioni di generazione Hash da sistema operativo Windows e OpenSSL.
- **Crittografia Asimmetrica e Certificati digitali** – Algoritmi Asimmetrici, Vantaggi e Svantaggi della Crittografia Asimmetrica, Esercitazioni di generazione chiavi pubbliche e private, crittografia e decrittografia con OpenSSL, Certificati digitali, CSR (Certificate Signing Request) con Windows e OpenSSL, Generazione Certificati e conversione del formato dei certificati.
- **Crittografia End-to-End** – Descrizione, Importanza, Vantaggi e Limiti, modalità di compromissione.
- **Mail Pec** – Approfondimento dell'utilizzo della crittografia, dei certificati digitali e della firma digitale.
- **Protocolli di Comunicazione Sicura** – SSH, SSL, TLS, Esercitazioni con OpenSSL.

## Obiettivo del corso

L'obiettivo del corso è quello di fornire ai partecipanti gli strumenti adeguati per:

- Capire il ruolo della Crittografia nella CyberSecurity;
- Comprendere i fondamenti della Crittografia;
- Gestire Certificati Digitali e Chiavi;
- Apprendere l'uso pratico degli strumenti;
- Saper applicare la Crittografia in contesti reali.

# Corso: Identity Security

**Titolo corso**
Identity Security

**Modalità di erogazione**
Sessione con docente da remoto oppure in presenza

**Motivazione del corso**
Il corso “Identity Security” introduce ed esplora il mondo delle identità digitali siano esse relative a persone che strumenti digitali, le relative problematiche e le soluzioni di gestione.

**Durata**
1..4 gg (modulabile in base alle esigenze)

**Destinatari**
CISO, resp. S.I., Amministratori di sistema

## Contenuto del Corso

- Introduzione all’Identity Security
- IAM - Access, MFA, Federation, Governance, SOD
- IAM - ABAC,RBAC, Differenze tra Identity e Access, SSO, Session and Token Management
- PAM1 - Perché PAM ? Cos’è PAM? , Conservazione sicura, Gestione
- PAM2 : Accesso, Audit, H2M, M2M, Cloud Ops, Identity Theft .

## Obiettivo del corso

L’obiettivo del corso è quello di fornire ai partecipanti la conoscenza delle tecniche di gestione delle identità digitali per una organizzazione, importanza della sicurezza delle identità nel attuale contesto digitale, le tipologie di strumenti disponibili per implementare tale gestione, e i rischi che derivano dalla mancata o insoddisfacente gestione delle identità digitali.

# Grazie

**www.exprivia.it**