



ISTITUTO TECNICO ECONOMICO
"AMBROGIO FUSINIERI"
VICENZA

Via G. D'Annunzio, 15 - 36100 VICENZA Tel. 0444563544 – Fax 0444962574 -
sito web: www.itefusinieri.gov.it E-mail: protocollo@itefusinieri.it - vild010003@pec.istruzione.it
Codice Fiscale 80016290241

Circolare n° 327

Agli studenti
Ai Docenti
Ai genitori degli alunni
Al personale ATA

Oggetto: *Corso NUOVA ECDL: IT-SECURITY SPECIALISED LEVEL per studenti, genitori, docenti, ATA.*

Con la presente si comunica che, nel mese di maggio, sarà attivato un corso pomeridiano gratuito di 10 ore, di preparazione al conseguimento della certificazione informatica NUOVA ECDL, relativo al modulo IT-SECURITY Specialised Level.

Il corso è riservato a coloro (studenti, docenti, personale ATA, genitori) che hanno acquistato – o acquisteranno entro la data d'inizio corso – la skill card e/o l'esame specifico, presso l'Istituto Fusinieri.

Il calendario degli incontri è il seguente:

DATA	ORARIO	LEZIONE
GIO 07/05/2015	14:00 – 16:00	1. CONCETTI DI SICUREZZA
LUN 11/05/2015	14:00 – 16:00	2. I MALWARE
GIO 14/05/2015	14:00 – 16:00	3. SICUREZZA IN RETE 4. USO SICURO DEL WEB
GIO 21/05/2015	14:00 – 16:00	5. COMUNICAZIONI 6. GESTIONE SICURA DEI DATI
LUN 25/05/2015	14:00 – 16:00	7. ESERCITAZIONI 8. SIMULAZIONE ESAME

Il calendario degli esami sarà oggetto di prossima circolare.

Si ricorda che il superamento del solo esame IT-Security dà diritto al conseguimento del rispettivo attestato.

Gli interessati sono pregati di comunicare la propria disponibilità ad iscriversi compilando il modulo allegato alla presente circolare e consegnandolo in portineria (alla sig.ra Rita o sig. Andrea).

Si coglie l'occasione per porgere cordiali saluti.

Vicenza, 27 aprile 2015

IL DIRIGENTE
Paolo Jacolino



ISTITUTO TECNICO ECONOMICO "AMBROGIO FUSINIERI"

Via G. D'Annunzio, 15 – 36100 VICENZA - Tel. 0444-563544 – Fax 0444-962574

E-mail: protocollo@itcfusinieri.it – vit010003@pec.istruzione.it

E-mail ecdl: ecdli@itcfusinieri.it Sito web: www.itefusinieri.gov.it

- programma del corso

MODULO PARTECIPAZIONE AL CORSO NUOVA ECDL, MODULO IT-SECURITY.

Il/La sottoscritto/a _____
Cognome _____ Nome _____

Data nascita: _____ Cod. fiscale: _____

Tel. _____ / _____ E-mail _____

SKILLS CARD n. _____ rilasciata da: _____

CHIEDE

di partecipare al corso per il conseguimento della certificazione NUOVA ECDL, modulo IT SECURITY .

Firma del Titolare della Skills card

Se minorenni firma del genitore:

Firma del genitore

E' possibile consultare la skills card e avere tutte le relative informazioni consultando il sito: <http://certificazioni.aicanet.it>

CORSO IT SECURITY

MODULO ECDL SPECIALISED LEVEL

INTRODUZIONE:

Poiché le tecnologie informatiche vengono utilizzate da un numero sempre crescente di persone per svolgere una gamma sempre più ampia di attività, diventa sempre più urgente la necessità di garantire la sicurezza dei dati.

Persone malintenzionate, infatti, possono accedere ad informazioni private che l'utente incautamente rende di dominio pubblico se non possiede le competenze e le conoscenze per impostare appropriati filtri, password e criteri di privacy.

Tutti gli utilizzatori di tecnologie informatiche dovrebbero vigilare sulle minacce alla sicurezza IT quali virus, phishing, hacker, frodi on-line e furti d'identità in generale.

L'uso di prodotti di sicurezza IT integrato con adeguate competenze e conoscenze, che consentono di identificare e affrontare le minacce alla sicurezza IT, è il modo più efficace per proteggere se stessi ed i propri dati.

OBIETTIVI DEL CORSO:

Il corso vuole fornire agli utenti le competenze e le conoscenze per riconoscere le minacce più comuni e intraprendere azioni preventive. Attraverso la capacità di individuare e comprendere i concetti principali alla base di un uso sicuro della Tecnologia dell'Informazione e Comunicazione (ICT) nella vita quotidiana, la conoscenza delle necessarie capacità e conoscenze per mantenere una rete di connessione sicura e dell'utilizzo di Internet, gli utenti del computer saranno quindi in grado di proteggere i propri dati e quelli dell'organizzazione per la quale lavorano. Certificare le competenze necessarie per identificare e affrontare minacce, quali il phishing e le transazioni fraudolente durante la navigazione sul Web e l'acquisto di beni e servizi online, può notevolmente migliorare la sicurezza online.

Il corso fornisce le conoscenze e le competenze necessarie per:

- identificare e trattare con la maggior parte delle minacce associate all'uso delle tecnologie informatiche
- affrontare l'esame del modulo ECDL IT Security - Specialised Level.

CONTENUTI DEL MODULO:

Il modulo IT SECURITY, oggetto del corso, definisce i concetti e le competenze fondamentali per comprendere l'uso sicuro dell'ICT nelle attività quotidiane e per utilizzare tecniche e applicazioni rilevanti che consentono di gestire una connessione di rete sicura, usare Internet in modo sicuro e senza rischi e gestire in modo adeguato dati e informazioni.

DURATA DEL CORSO:

10 ore di teoria.

5 ore di pratica.

PROGRAMMA DETTAGLIATO DEL CORSO:

1.1 CONCETTI DI SICUREZZA

2. Dati e informazioni
3. Il crimine informatico
4. Hacking, cracking e hacking etico
5. Riconoscere le minacce ai dati
6. Proteggere le informazioni personali
7. Prevenire accessi non autorizzati ai dati
8. Confidenzialità, integrità, disponibilità delle informazioni
9. Protezione, conservazione e controllo dei dati
10. Le linee guida e politiche per l'uso dell'ICT
11. L'Ingegneria sociale
12. I metodi applicati dall'ingegneria sociale
13. Il furto di identità
14. Il fenomeno dello skimming
15. Attivare e disattivare le impostazioni di sicurezza delle macro
16. Impostare una password ad un file di testo
17. Impostare password su file compressi

1.2 I MALWARE

1. Che cosa è un malware e come funziona
2. Tipologie di malware: (Trojan, Rootkit, Backdoor, Virus, Worm).
3. Furto di dati ed estorsioni: Adware, Spyware, Botnet, Keylogger, Dialer
4. Programmi anti-virus
5. Il processo di scansione
6. Virus in quarantena

1.3 SICUREZZA IN RETE

2. Che cosa è una rete informatica
3. Riconoscere i più comuni tipi di rete
4. L'amministratore di rete
5. Come connettersi a una rete
6. Il firewall
7. La sicurezza in rete
8. Connettersi ad una rete wireless
9. Sicurezza per reti senza fili
10. L'account di rete
11. La gestione della password
12. Le tecniche biometriche a sostegno della sicurezza in rete

1.4 USO SICURO DEL WEB

1. Riconoscere i siti sicuri
2. Riconoscere i rischi
3. Rendere sicura la navigazione
4. Reti sociali

1.5 LE COMUNICAZIONI ON-LINE

1. La cifratura dei messaggi di posta elettronica
2. La Firma Digitale
3. Apposizione della Firma Digitale
4. Messaggi fraudolenti e non richiesti
5. Che cosa è il phishing
6. Elementi caratterizzanti il phishing
7. I rischi della posta elettronica
8. Messaggistica istantanea
9. I limiti di sicurezza della messaggistica istantanea
10. Confidenzialità delle informazioni

1.6 GESTIONE SICURA DEI DATI

1. Assicurare l'integrità di dati e dispositivi
2. Il Backup
3. Effettuare un Backup
4. Eseguire il ripristino dei dati
5. Cancellazione sicura dei dati

DOCENTE

Salvatore Marcello Imbesi