



La presente comunicazione, trasmessa solo VIA FAX, sostituisce l'originale ai sensi dell'art 6, comma 2, Legge n. 412/1991

Sede legale: Via G. Cusmano, 24 - 90141 PALERMO
C.F. e P. I.V.A.: 05841760829

Palermo : 17 DIC. 2015
Prot. N. 11994

Dipartimento Provveditorato e Tecnico
U.O.S. Servizio Informatico Aziendale e Gestione
Collegamenti
Via Pindemonte, 88 - 90129 Palermo
Telefono: 091 703.3309 Fax: 091 703.3038
E-mail servizioinformatico@asppalermo.org
WEB : www.asppalermo.org

Direzione Generale
Direzione Amministrativa
Direzione Sanitaria

FAX A Direttore P.O. Dei Bianchi di Corleone
Direttore P.O. Madonna dell'Alto Petralia Sottana
Direttore P.O. Civico di Partinico
Direttore P.O. "Ingrassia", Palermo
Direttore P.O. "Cimino" di Termini Imerese
Direzione U.O.C. Coordinamento Staff Strategico
Direttore U.O.C. Organizzazione e Programmazione delle Attività di Cure Primarie
Direttore Risorse Economico-Finanziarie e Patrimoniale
Direttore Risorse Umane, Sviluppo Organizzativo e Affari Generali
Direzione Dipartimento di Prevenzione
Direttore Dipartimento Prevenzione Veterinario
Direttore Dipartimento Salute Mentale, Dipendenze Patologiche e Neuropsichiatria dell'Infanzia e dell'Adolescenza fax 091-7033068
Direttore Attività Territoriali e Integrazione Socio-Sanitaria Direttore U.O.S. Servizio Prevenzione e Protezione Fax 091-703-3053

Ai Direttori dei Distretti di:

- 42: Palermo
- 41: Partinico
- 40: Corleone
- 37: Termini Imerese
- 36: Misilmeri
- 35: Petralia Sottana
- 33: Cefalu'

Ai Direttori dei Poliambulatori di:

- Palermo Centro
- Palermo Aiuto Materno
- Palermo Biondo
- Palermo Pozzillo
- Palermo Guadagna

Direzione Dipartimento di Ospedalità Pubblica
Direzione Dipartimento Ospedalità Privata
Direzione Dipartimento Diagnostica di Laboratorio
Direzione Dipartimento Screening Mammografico
Direzione Dipartimento di Diagnostica Per Immagini
Direzione Ufficio Invalidi Civili

Oggetto : Virus Informatici

Da pochi giorni diverse aziende sono state attaccate da un virus chiamato Cryptolocker

Questo virus, la cui modalità di propagazione avviene, nella maggior parte dei casi, mediante apertura di un file pdf allegato ad una e-mail che sembra indirizzata a noi (phishing), cifra in modo silente tutti i file del computer.

Cifra anche i file che sono contenuti nei dispositivi collegati al computer, ossia chiavette usb, hard disk esterni, memorie rimovibili, cartelle condivise, per cui tali dispositivi sono comunque da considerare ad elevato rischio.

L'antivirus Microsoft (Microsoft Security Essentials) che è installato di norma sui nostri pc, nonché gli altri Antivirus Commerciali, sono in grado di riconoscere questo virus, ma, per motivi di "propagazione dell'infezione" non sono in grado di riconoscere le varianti più recenti (solitamente quelle che vengono create dagli hacker nelle ultime due o tre settimane".

Similmente a quanto succede nell'Uomo, i Virus informatici hanno un periodo di incubazione più o meno lungo, nella quale non mostrano alcun segno della loro presenza e cercano di propagarsi in modo silente.

Gli antivirus, durante tale periodo ed in generale sino a che i file sospetti non vengono inviati in laboratorio, non sono in grado di riconoscere tali virus ed essenzialmente li lasciano transitare e/o agire in modo indisturbato.

Ciò porta alla evidente considerazione che **non esiste un antivirus che riconosca tutti i virus presenti in circolazione, soprattutto se recentissimi**, vi è invece la possibilità che qualche antivirus (solitamente quelli più installati e/o con funzioni euristiche evolute) venga aggiornato più velocemente e quindi riconosca il virus qualche giorno, o qualche settimana, prima degli altri antivirus.

Ovviamente, **è buona norma**, al fine di evitare infezioni, **non solo non aprire e-mail sospette o con contenuti o informazioni a noi non destinate ma anche non visitare siti non istituzionali.**

A prescindere dai tempi di individuazione dell'infezione e dalla cura della stessa, e' fondamentale anzi perentorio, fare il backup periodicamente dei vostri dati (almeno una volta alla settimana) su supporti non cancellabili (CdRom o DVD) e/o su supporti rimovibili (penne usb, Hard disk esterni, memorie, etc) **che a fine backup devono essere rimossi e conservati** in luogo sicuro.

Tale prassi, è valida non solo per recuperare dati attaccati o danneggiati dai virus, ma anche per ripristinare gli stessi nel caso di guasto dell'hard disk o del dispositivo di memorizzazione in uso sul pc.

Si raccomanda quindi il periodico salvataggio dei propri dati, avendo cura di effettuarlo periodicamente su più supporti e di mantenerne copia per almeno 4/8 settimane.

Con preghiera di massima diffusione

*Il Responsabile dell' U.O.S. Informatica Aziendale
(Ing. Stefano Serra)*



Il Direttore del Dipartimento Provveditorato e Tecnico

(Avv. Damiani Fabio)

