NOTA STAMPA

Il Giubileo è a prova di hacker con i consigli di ESET

Il decalogo di ESET per sopravvivere nella giungla delle reti Wi-Fi pubbliche romane ed evitare il furto dei dati personali

Roma, 10 novembre 2015 – Il Giubileo di Papa Francesco è ormai alle porte e la città di Roma si appresta ad ospitare milioni di pellegrini e turisti provenienti da tutto il mondo, che faranno un ampio utilizzo dei propri computer e dispositivi mobili nei luoghi di pellegrinaggio, negli hotel e nei principali punti di interesse della città. Un'occasione ghiotta questa per i pirati informatici, pronti a sfruttare la cassa di risonanza di un evento così importante per infiltrarsi nelle migliaia di reti Wi-Fi pubbliche romane e avere facile accesso ai dati sensibili di pellegrini e turisti. I ricercatori di ESET®, il più grande produttore di software per la sicurezza digitale dell'Unione Europea, hanno dunque stilato un decalogo per vivere in tutta sicurezza il Giubileo e navigare sulle reti Wi-Fi pubbliche evitando il furto delle informazioni personali e delle carte di credito:

1. ***Verificate l'autenticità della rete*** - Chiedete sempre al proprietario della rete Wi-Fi il nome esatto della rete e della password e siate molto cauti se non ci sono le password WPA o WPA2 per l'accesso protetto al Wi-Fi, in quanto ciò significa che la connessione è in chiaro. Prestate molta attenzione ad hotspot potenzialmente contraffatti che hanno nomi strettamente somiglianti a quelli ufficiali.
2. ***Cercate gli HTTPS*** - E' importante assicurarsi che le pagine web visitate siano codificate in HTTPS, ove possibile; basta cercare il codice HTTPS all'inizio della stringa dell'URL o verificare la presenza nella stessa posizione di un segno di lucchetto di sicurezza. Questo indica che il sito web, e in particolare la pagina che state visitando, dispone di un certificato digitale valido e di un sistema aggiornato di crittografia SSL / TLS, che rende gli attacchi Man- in-the - Middle (MITM) molto meno probabili. Attenzione ai siti mobile, poiché per questi non c'è nessuna garanzia che siano in HTTPS.
3. ***Patch prima di partire***! - L'installazione delle patch e l'aggiornamento del software su base regolare è una pratica di sicurezza indispensabile, soprattutto quando si naviga su connessioni Wi-Fi. I pirati informatici spesso approfittano dei mancati aggiornamenti per ingannare gli utenti ignari inducendoli a scaricare falsi aggiornamenti software. I ricercatori di ESET consigliano di tenere sempre aggiornati i browser ed i software antivirus per rilevare e rimuovere anche le minacce più recenti.
4. ***Evitate l'accesso alle informazioni sensibili tramite reti Wi-Fi -*** E' buona norma non utilizzare le reti Wi-Fi pubbliche per accedere alla propria posta elettronica, al proprio sito di home banking o all'account relativo alle carte di credito.
5. ***Selezionate manualmente la rete Wi-Fi*** - Assicuratevi che i vostri laptop, smartphone o dispositivi portatili siano impostati per selezionare manualmente una rete wireless e non per una connessione automatica. Gli esperti di ESET suggeriscono inoltre di far "dimenticare" al dispositivo le reti Wi-Fi

che non si utilizzano spesso, per evitare le connessioni automatiche quando queste si trovano nuovamente a portata di segnale.

6. ***Utilizzate una VPN*** **-** Prendete in considerazione una rete privata virtuale (VPN), uno dei modi più sicuri per navigare in Internet in maniera criptata. Le soluzioni VPN forniscono crittografia e sicurezza nelle reti pubbliche, mascherando il proprio indirizzo IP e riducendo in questo modo le opportunità di cadere nella trappola del phishing.
7. ***Utilizzate strumenti di sicurezza aggiuntivi*** - C'è ormai una grande attenzione alla privacy online e strumenti come Tor, VPNs e DoNotTrack sono diventati sempre più popolari. A proposito delle reti pubbliche Wi-Fi è possibile trovare estensioni utili a forzare la crittografia di siti web che non sono crittografati per impostazione predefinita. Questo non vi proteggerà su tutti i siti, ma su molti sarà efficace.
8. ***Adottate una 2FA*** **-** Abilitate l'autenticazione a due fattori, dove possibile. Il 2FA è sempre più visto come il futuro dell'autenticazione, ed è saggio abilitarlo per chiunque utilizzi un hotspot, aggiungendo un ulteriore livello di protezione.
9. ***Effettuate il logout quando avete concluso la sessione online*** **-** Non mantenete sempre attivo il login ai vostri account personali quando siete collegati ad hotspot Wi-Fi, perché questo potrebbe esporvi agli attacchi degli hacker. Per maggiore sicurezza, eseguite il logout da ogni sito dopo ogni sessione.
10. ***Spegnete il Wi-Fi se non lo utilizzate*** **-** Se volete essere al sicuro e non state utilizzando Internet è meglio spegnere il Wi-Fi, azione estremamente facile sia con Windows che con OS X; più infatti rimarrete visibili online, più attirerete l'attenzione di gente curiosa e pronta ad "importunarvi".

Ufficio Stampa: Elisabetta Giuliano
Email: elisabettagiuliano@yahoo.it
Mobile: 328.9092482

ESET, fondata nel 1992, è uno dei fornitori globali di software per la sicurezza informatica di pubbliche amministrazioni, aziende e utenti privati. Il software ESET NOD32 Antivirus fornisce una protezione in tempo reale da virus, worm, spyware e altri pericoli, conosciuti e non, offrendo il più elevato livello di protezione disponibile alla massima velocità e con il minimo impiego di risorse di sistema. NOD32 è l'antivirus che ha vinto il maggior numero di certificazioni Virus Bulletin 100% e dal 1998 non ha mai mancato l'individuazione di un virus ItW (in fase di diffusione). ESET NOD32 Antivirus, ESET Smart Security e ESET Cybersecurity per Mac rappresentano le soluzioni per la sicurezza informatica più raccomandate a livello mondiale, avendo ottenuto la fiducia di oltre 100 milioni di utenti. L'azienda, presente in 180 Paesi, ha il suo quartier generale a Bratislava e uffici e centri di ricerca a San Diego, Buenos Aires, Singapore, Praga, Cracovia, Montreal, Mosca. Per quattro anni di seguito ESET è stata inclusa fra le aziende Technology Fast 500 EMEA da Deloitte e per dieci anni consecutivi fra le aziende Technology Fast 50 Central Europe. Per maggiori info: **www.eset.it**

FUTURE TIME è il distributore esclusivo dei prodotti ESET per l'Italia, nonché suo partner tecnologico. Fondata a Roma nel 2001, Future Time nasce dalla sinergia di due preesistenti aziende attive da anni nel campo della sicurezza informatica. Future Time, con Paolo Monti e Luca Sambucci, fa parte della **WildList Organization International**, ente no profit a livello mondiale composto da esperti e aziende antivirus che hanno il compito di riportare mensilmente tipologia e numero dei virus diffusi in ogni Paese. Per maggiori info: **www.eset.it**