faronotizie.it
Webmagazine internazionale di informazione

ANNO XIX – N° 224 – Dicembre 2024

Password, Pin, Puk, Spid...

Editoriale del direttore Giorgio Rinaldi

Sino a qualche anno fa, le parole password, pin, puk, spid ed altre simili amenità erano, ai più, delle perfette sconosciute.

Come la maggior parte delle soluzioni informatiche, l'invenzione si deve ai militari, che più d'ogni altri hanno necessità di agire nel massimo della segretezza e della sicurezza, specialmente nelle comunicazioni.

Ai tempi dell'impero romano, i legionari usavano come mezzo di identificazione le parole d'ordine (*tessera*); poi, con l'avvento delle comunicazioni criptate, sono entrate in auge delle particolari parole che hanno la funzione di chiave per aprire le serrature dei luoghi virtuali dove custodiamo informazioni che devono mantenersi celate a chi non ne ha diritto.

Man mano che l'"Era Digitale" sovvertisse le società mondiali, le password vennero utilizzate dapprima (decennio 1960/70) con i sistemi di computer condivisi (p.es.: il CTSS); poi (1970/80), con la diffusione dei personal computer, i protocolli di rete (Telnet e FTP) iniziarono massicciamente l'uso delle password per accedere ai sistemi remoti; dal 1990, e la diffusione esponenziale di internet, le password sono diventate essenziali per la protezione dei propri dati.

Alla inarrestabile ricerca e utilizzo di password sempre più complesse, si unì anche il progetto di un codice numerico detto PIN (Personal Identification Number), breve e facile da ricordare che dal 1967 è entrato nelle attività delle banche con il bancomat, e da qui ai telefoni cellulari e congegni elettronici vari.

Quale ulteriore aiuto alla sicurezza dei propri dati, è stato affiancato il PUK (Personal Unblocking Key), un codice specifico utilizzato per sbloccare dispositivi non più idonei per l'inserimento errato del Pin.

Il puk un codice di otto cifre elaborato dai sistemi informatici dell'operatore e non modificabile dal cliente.

Negli anni 2000 l'Italia ha iniziato ad investire nella digitalizzazione della Pubblica Amministrazione.

Già dal 2005 il CAD (Codice dell'Amministrazione Digitale) aveva previsto strumenti per favorire e incentivare la digitalizzazione, ma il tutto era sempre frammentato tra diverse realtà.

L'Agenda Digitale Europea (2010) ha indotto l'Italia a sviluppare un sistema unificato.

Nel 2013 viene approvato il progetto Spid che viene affidato all'Agenzia per l'Italia Digitale (AgID).

Nel marzo 2016 Lo Spid diventa operativo e vengono autorizzati i primi tre *identity provider*: InfoCert, Poste Italiane e Tim.

Nel 2021 lo Spid diventa obbligatorio per accedere alla maggior parte dei servizi online della Pubblica Amministrazione.

I livelli di Sicurezza dello SPID sono tre: offre tre livelli di sicurezza: livello 1: Accesso con username e password; livello 2: Autenticazione a due fattori (es. OTP via SMS o app); livello 3: Accesso con strumenti di crittografia avanzata.

Da ultimo, si è aggiunta la CIE (Carta di Identità Elettronica) che è un'alternativa allo Spid per l'autenticazione digitale.

Tutti gli sforzi degli esperti informatici nostrani non hanno prodotto, però, i risultati sperati: i sistemi sono vulnerabili, ancorché complicati e, inoltre, ignorano una fascia sostanziosa della popolazione più adulta, non adusa alle bizzarrie dei fornitori.

Quelli che si occupano di informatica, ricordano tanto dei fantomatici venditori di automobili Ferrari che hanno una clientela composta solo da neopatentati.

L'ostinazione ad elaborare sistemi che non tengono conto delle capacità delle persone alle quali sono rivolti, non può che produrre un rallentamento alla digitalizzazione dei servizi pubblici e privati.

E, questo quando i produttori sono affidabili.

La mia esperienza quotidiana con lo Spid fornito da un *identity provider* famoso, mi ha costretto ad utilizzare, ove possibile, altre strade, vista la sua totale quanto prevedibile inaffidabilità.

In sintesi, dei finti esperti hanno elaborato sistemi complicati e distanti anni luce dalle esigenze dei cittadini.

A molti, invece di rendere la vita più semplice, gliel'hanno solo complicata: password con una lettera maiuscola, minimo 8 cifre, almeno un numero ma non due consecutivi, un segno grammaticale etc; numero a tergo segreto, parola d'ordine, domanda di riserva: chi era il/la tuo/a maestra/o alle elementari?; codice sms; codice otp.

E, questa baraonda di pin, pass e altre diavolerie, di cui bisogna prendere nota per iscritto (ma nascondendo i bigliettini dove sono stati trascritti i codici, che dopo un po' diventano introvabili o illeggibili), è stata adottata da qualunque azienda, così anche per andare al supermercato e comprare un prodotto in sconto devi avere una tessera con tutti i suoi bravi *username* e *password*.

Per non dire delle famigerate "App.": anche solo scaricarne una sul cellulare per, magari, le previsioni del tempo, occorre registrarsi e creare un account con *username*, *password*, e-mail, numero di cellulare e poi ri-accedere con il codice inviato via sms al telefonino modello x con numero seriale y…

Ultimamente, ti costringono ad essere utente anche di piattaforme cosiddette "social", con relativi *account* e *password* d'accesso, altrimenti non puoi andare oltre … nelle previsioni meteorologiche!

Non solo, quindi, devi ricordare o scriverti centinaia di nomi di accesso e complicate combinazioni "alfanumerichesimboliche", ma devi conoscere anche la lingua inglese ed essere un fan di "social": un vero trionfo dell'idiozia e di tecnici

incapaci di trovare, dopo decenni, chiavi d'accesso sicure e semplici allo stesso tempo.

Il premio Nobel dell'assurdo spetta alle Poste Italiane: mi hanno bloccato l'accesso al livello 3; per ripristinarlo, dopo lunga ricerca nel sito delle Poste, occorre indicare un codice che mi hanno inviato qualche anno fa via sms, altrimenti andare di persona in un loro ufficio e chiederne uno nuovo, anche se ti trovi all'estero o allettato...

Un bel passo avanti, e due indietro.