Istituto Nazionale di Fisica Nucleare
SEZIONE DI FIRENZE
Servizio Calcolo e Reti

Sicurezza nell'uso della rete e della posta elettronica

Introduzione

Non esiste una ricetta unica e definita per eliminare tutti i rischi legati alla sicurezza informatica.

Questa guida ha lo scopo di fornire solo alcune informazioni ed indicazioni di comportamento per cercare di ridurre tali rischi e comunque non sostituisce i seguenti documenti di riferimento dell'Ente e del GARR[1]:

- Disciplinare per l'uso delle risorse informatiche nell'INFN (24/01/2020);
- Modulo di implementazione delle misure minime di sicurezza nell'Istituto Nazionale di Fisica Nucleare (20/12/2017) e relative norme d'uso
  - per sistemi operativi Linux,
  - per sistemi operativi Microsoft Windows,
  - per sistemi operativi Mac;
- Acceptable Use Policy (AUP) GARR (06/11/2017).

Tutte le indicazioni fornite e le norme di comportamento proposte, sia sotto forma di semplici consigli che come necessità vincolanti da rispettare, sono da considerarsi una soluzione di compromesso applicabile a singoli problemi di sicurezza nel maggior numero di casi ed al maggior numero di utenti. In altre parole, anche per non creare confusione, verranno date indicazioni precise e per lo più univoche nell'affrontare i singoli problemi di sicurezza senza lasciare spazio ad eventuali altre soluzioni altrettanto valide ma magari applicabili a situazioni o utenti particolari. Se i singoli utenti valutano di avere una conoscenza e un'esperienza di questi argomenti tale da permetter loro di applicare soluzioni alternative lo faranno ovviamente prendendosi la totale responsabilità delle loro scelte.

1 GARR (acronimo di Gruppo per l'Armonizzazione della Rete della Ricerca) è il nome della rete italiana a banda ultra-larga dedicata alla comunità dell'istruzione, della ricerca e della cultura. Concepita negli anni '80, e realizzata nel 1991, è gestita dal Consortium GARR, fondato nel 2002. I soci fondatori sono: Consiglio Nazionale delle Ricerche, ENEA, Istituto Nazionale di Fisica Nucleare e Conferenza dei Rettori delle Università Italiane in rappresentanza di tutte le università italiane.

Il problema della sicurezza informatica

Durante l'attività lavorativa, ma non solo, utilizziamo continuamente *"web browser"*[2], *"mail client"*[3] e applicazioni di rete per accedere a risorse presenti su Internet. Per questo dobbiamo aver ben presente che la rete è fortemente popolata da malintenzionati e da vere e proprie associazioni criminali che, tramite strumenti sempre più potenti, cercano di attaccare le risorse informatiche di associazioni, organizzazioni, enti, aziende o altro per danneggiarle o trarne un profitto in modo illegale.

Per la Sezione INFN di Firenze ed in generale per l'intero INFN, i maggiori pericoli attuali legati a queste attività criminali sono:

- la possibilità di cadere in vere e proprie truffe con ingenti danni economici per l'Ente;
- la possibilità di sottrazione, modifica o cancellazione di dati personali o comunque riservati con conseguenti ricatti o esposizione a problemi legali, denunce e sanzioni economiche per l'Ente;
- la cifratura di dati[4] presenti sia sui singoli PC[5] utilizzati nell'attività lavorativa giornaliera che sui *server*[6] che offrono servizi di rete e la conseguente richiesta di un riscatto per poter ottenere la chiave con cui recuperare i dati.

La posta elettronica (o *"e-mail"* o semplicemente *"mail"*) è uno degli strumenti informatici più utilizzati sia in termini di numero di utenti che in termini di quantità di tempo che ogni utente dedica al suo utilizzo. Per questo motivo la posta elettronica rappresenta potenzialmente il mezzo più idoneo sia per la diffusione di *"malware"*[7] che per carpire informazioni preziose o credenziali.

Oltre all'enorme bacino di utenza, un aspetto che rende questo strumento sempre più appetibile ai numerosissimi malintenzionati che popolano la rete è la semplicità di utilizzo che questo mezzo ha raggiunto. Infatti, per rendere la vita dell'utente sempre più semplice, gli strumenti che usiamo per leggere le *e-mail* implementano automatismi sempre più efficaci e proprio per questo sempre più pericolosi. Ad esempio, alcuni *mail client* possono essere configurati per visualizzare automaticamente l'anteprima dei documenti allegati alle *e-mail*. Questa semplice funzione, che può risultare molto comoda per l'utente, nasconde il pericolo di poter eseguire del codice

2 Un *web browser*, o semplicemente *browser*, è un'applicazione *software* (un programma) che consente agli utenti di navigare e interagire con le risorse presenti su Internet. È uno strumento fondamentale per accedere e visualizzare pagine *web*, file multimediali, documenti, servizi online e altre risorse disponibili sulla rete. Esempi di browser web sono: Mozilla Firefox (Windows/macOS/Linux), Google Chrome (Windows/macOS/Linux), Chromium (Windows/macOS/Linux), Safari (macOS), Microsoft Edge (Windows/macOS), Brave (Windows/macOS/Linux), Vivaldi (Windows/macOS/Linux), ecc.

3 Un *mail client* (in italiano "agente di posta elettronica") è un'applicazione *software* (un programma) che consente agli utenti di inviare, ricevere e gestire i messaggi di posta elettronica. Si tratta di un *software* installato nel proprio PC che consente di accedere alle caselle di posta elettronica tramite un'interfaccia grafica. Esempi di client di posta elettronica sono: Mozilla Thunderbird (Windows/macOS/Linux), Microsoft Outlook (Windows/macOS), Apple Mail (macOS), ecc.

4 La cifratura dei dati è un processo attraverso il quale le informazioni vengono trasformate da una forma leggibile e comprensibile (testo in chiaro) in una forma incomprensibile (testo cifrato). Il processo di cifratura coinvolge l'uso di un algoritmo crittografico e una chiave. L'algoritmo crittografico determina come i dati vengono manipolati per renderli incomprensibili, mentre la chiave è un valore segreto utilizzato dall'algoritmo per eseguire questa manipolazione. Noto l'algoritmo di cifratura, solo chi possiede la chiave corretta può decifrare i dati cifrati e ripristinarli alla loro forma originale.

5 *"Personal Computer"*: computer fissi da tavolo (*"desktop"*) e computer portatili (*"laptop"*).

6 Un *server* è un computer o un sistema informatico dedicato a fornire servizi di rete ad altre apparecchiature (PC, *tablet*, *smartphone*, altri *server*) detti *client*. Per esempio un *web server* mette a disposizione pagine *web* contenenti immagini, file, dati e altre risorse consultabili tramite *client* detti *web browser*; un *mail server* gestisce i messaggi di posta elettronica a cui un utente accede tramite un *mail client*.

7 Con il termine *malware* (abbreviazione per *"malicious software"*, che significa letteralmente "software malintenzionato", ma di solito tradotto come "software dannoso") si indica un qualsiasi programma informatico usato per disturbare le operazioni svolte da un utente di un computer. I *malware* sono caratterizzati dall'intento doloso dei loro creatori e si classificano in varie categorie a seconda del metodo con cui si diffondono o del loro comportamento: virus, worm, trojan horse, backdoor, spyware, dialer, hijacker, rootkit, scareware, rabbit, adware, malvertising, keylogger, rogue antispyware, ransomware, ...

eventualmente nascosto nei messaggi di posta e quindi essere veicolo di compromissioni delle postazioni di lavoro o degli *"account"*[8] ad esse collegati.

Ciascun utente deve prendere coscienza che l'uso non appropriato della rete, dei propri *account* ed in particolare del proprio *account* di posta elettronica può comportare gravissimi danni, anche in termini economici, non solo al proprio lavoro e alla propria persona ma anche ai colleghi e all'intero Ente.

Ingenuamente un utente potrebbe infatti pensare che l'unico aspetto critico nella gestione dei propri *account* e della posta elettronica sia legato all'eventuale diffusione di dati di lavoro o personali contenuti nei messaggi di posta o nei PC che utilizza. Questa eventualità è di per sé un aspetto gravissimo in quanto espone l'Ente a eventuali denunce e sanzioni economiche ed inoltre tali dati, che possono esser considerati erroneamente di scarso valore da parte dell'utente, possono esser utilizzati da malintenzionati per affinare e migliorare il livello di un attacco informatico. Ma i problemi non si limitano solo a questo, infatti poter controllare un account di posta elettronica permette:

- di inviare richieste o contenuti falsi a destinatari che, ovviamente, riconosceranno tali messaggi come autentici;
- di depositare nella casella di posta della vittima messaggi falsi che l'utente non può in nessun modo distinguere da quelli autentici;
- di inviare *malware* a colleghi, amici, parenti o altro con maggiore probabilità di essere eseguiti;
- di inviare messaggi con maggiore probabilità di superare i filtri di posta e quindi di inviare messaggi di *"phishing"*[9] con maggiore probabilità di trarre in inganno i destinatari, cioè fare *"escalation"*[10] verso vittime con responsabilità amministrative o dirigenziali;
- di compromettere il servizio di posta elettronica di tutta la Sezione o dell'intero Ente;
- di realizzare vere e proprie truffe.

Solo un uso consapevole da parte degli utenti della rete, dei propri *account* ed in particolare del proprio *account* di posta elettronica riduce in modo consistente la probabilità di essere vittime, e allo stesso tempo inconsapevolmente complici, di attività illecite o attacchi informatici (*spam*[11], *phishing*, *malware*, compromissioni, truffe o altro).

8 Un *account* è un insieme di informazioni e credenziali (coppia *"username"* e *"password"*) che permettono a una persona di accedere a un sistema informatico o a un servizio di rete. Solitamente oltre alle credenziali sono contenute altre informazioni come, per esempio, indirizzo email, numero di telefono, nome, cognome, data di nascita, ecc. Gli *account* sono utilizzati per identificare e autenticare gli utenti, consentendo loro di accedere a risorse protette o a funzionalità specifiche all'interno di un sistema, un'applicazione o una piattaforma web.

9 Consultare una delle sezione successive per una descrizione delle tecniche di *phishing*.

10 In ambito di sicurezza informatica con *escalation* si intende un qualsiasi processo che, a partire da un account non particolarmente privilegiato, permette di acquisire privilegi via via crescenti fino a raggiungere livelli tali da poter permettere a malintenzionati di effettuare operazioni impreviste e non autorizzate. In particolare con *"privilege escalation"* si intende lo sfruttamento di un errore di un utente, di una falla, di un errore di progetto o di configurazione di un *software* o di un sistema operativo al fine di acquisire il controllo di risorse normalmente precluse ad un utente o ad un'applicazione.

11 Con il termine *spam* si intende una pratica indesiderata e fastidiosa di invio di messaggi non richiesti e di massa, tipicamente attraverso *e-mail*. Gli *spammer* inviano queste comunicazioni in modo indiscriminato a un gran numero di destinatari, senza il loro consenso, con l'obiettivo di diffondere pubblicità indesiderata, promuovere prodotti o servizi, diffondere truffe, *malware* o ottenere informazioni personali o finanziarie delle persone.

Schema ricorrente di truffe o di attacchi alle Amministrazioni

Sempre più frequentemente le Amministrazioni sono oggetto di truffe realizzate secondo il seguente schema o simili.

1. Vengono rubate le credenziali della posta di un utente. È particolarmente pericoloso se si tratta di un un utente con responsabilità amministrative, dirigenziali o che comunque è coinvolto in acquisti e gestione dei fondi ma anche altri utenti possono essere utilizzati per fare *"escalation"* ed arrivare ad utenti con ruoli critici in un secondo momento.
2. Vengono lette tutte le mail dell'utente senza nessuna azione che segnali la compromissione dell'account (nessuno si accorge di niente).
3. Al momento opportuno, solitamente mentre è in corso un acquisto di un oggetto costoso, viene confezionata una mail per la vittima in cui si indica di fare un pagamento su un certo conto. La mail è confezionata bene perché riporta tutti i dettagli relativi all'ordine in corso, alla procedura d'acquisto, alla ditta e alle persone coinvolte con tutti i dettagli che fanno intendere che sia una mail reale ed in più si configura spesso come una risposta ad un mail reale di cui viene citato il testo, magari scritta in precedenza proprio dalla stessa vittima. A volte, ma non necessariamente, vengono aggiunti aspetti di pressante necessità e di emergenza in modo da aumentare la pressione psicologica sulla vittima.
4. La vittima, convinta che i riferimenti indicati siano giusti, fa il pagamento per l'oggetto che è stato realmente ordinato sul conto bancario aperto appositamente per la truffa e con proprietario difficilmente rintracciabile.
5. Incassato il pagamento, il conto viene chiuso.

Purtroppo quanto descritto avviene realmente e sempre con maggiore frequenza in ambienti sempre più vicini all'INFN come pubbliche amministrazioni, enti pubblici, università, enti di ricerca se non addirittura proprio nell'INFN stessa.

Il tutto consiste nel riuscire ad entrare nell'*account* di posta elettronica della vittima, quindi nell'impossessarsi delle credenziali del suo *account* di posta elettronica per poi poter leggere i messaggi e poter depositare la *mail* fasulla per portare a termine la truffa.

È importante sottolineare che i truffatori, essendo in possesso di *username* e *password* della posta elettronica della vittima che effettuerà il pagamento o di un suo collega possono generare un mail che nessuno può identificare come falsa: sia i destinatari che i sistemi di protezione e filtraggio della posta identificheranno tale *mail* come autentica, perché di fatto lo è.

1. Se vengono rubate le credenziali dell'*account* di posta elettronica di un dipendente che può effettuare pagamenti, la *mail* di truffa viene depositata direttamente nel suo *account* senza passare dai filtri per il blocco di *spam* e *malware*; in altre parole la vittima è completamente in balia dei truffatori e non può in nessun modo rendersi conto che la *mail* è fasulla. Soltanto da un'attenta analisi dei *log*[12] dei *server* di posta si potrà vedere che tale *mail* non ha transitato attraverso gli usuali canali di recapito della posta elettronica ma è stata depositata direttamente nel *mail server*; tale analisi può essere effettuata solo a posteriori sapendo cosa cercare.
2. Se invece vengono rubate le credenziali dell'account di posta elettronica di un utente coinvolto nella procedura d'acquisto, la mail di truffa viene inviata dal suo account e anche in questo caso sia i sistemi di filtraggio che i destinatari riconosceranno tale mail come autentica.

12 Un *log* è un insieme di dati, solitamente salvati in un *file* o in un qualsiasi registro, che riportano e conservano informazioni dettagliate sugli eventi o sulle attività che si verificano in un sistema informatico, in un'applicazione o in un dispositivo.

Il problema non riguarda solo chi effettua pagamenti (Servizio Amministrazione) ma tutti gli utenti che gestiscono ordini (Magazzino, Servizio Tecnico, RUP) o dati particolari (Servizio di Direzione) perché tutti i dati relativi a dipendenti, associati, ordini e fornitori possono essere utilizzati per fare *escalation* verso *account* critici per effettuare truffe.

Parallelamente esiste anche il problema dei *"ransomware"*: programmi, spesso diffusi tramite posta elettronica o chat o piattaforme social, con cui vengono criptati tutti i dati presenti sul PC della vittima. Dopo che tutti i dati sono stati criptati viene richiesto un riscatto per avere la chiave per accedere nuovamente ai propri dati. In caso di *ransomware* si deve aver ben presente che non vengono criptati solo i dati presenti fisicamente nelle memorie (*hard disk*) del PC infettato ma anche tutti i *file* presenti su tutte le risorse di rete a cui il PC ha accesso: potenzialmente i *backup*, la posta elettronica, i *file* depositati su google drive, microsoft onedrive, seafile, owncloud, netcloud, dropbox, ecc.

La considerazione "se mi rubano le mie *password* poco male, tanto a chi vuoi che interessino le mie *mail* o il mio *account* INFN-AAI!" purtroppo è completamente sbagliata: i bilanci dell'INFN sono pubblici e con cifre che sicuramente risultano molto appetibili per la criminalità organizzata. Inoltre i più recenti attacchi a Pubbliche Amministrazioni, per esempio alla Regione Lazio nel 2021, alla sanità di Padova nel 2022, alla sanità dell'Abruzzo nel 2023, e moltissimi altri sono stati realizzati a partire dal furto di credenziali di semplici utenti non privilegiati equivalenti ad un qualsiasi dipendente INFN o ad un qualsiasi associato.

URL

Una URL, acronimo di *"Uniform Resource Locator"* (in italiano, localizzatore uniforme di risorse), è un indirizzo univoco che identifica la posizione di una risorsa su Internet. È una sequenza di caratteri che viene utilizzata per specificare l'indirizzo di una pagina *web*, una piattaforma *web*, un *file*, un'immagine, un video o qualsiasi altra risorsa disponibile su Internet.

Un qualsiasi *web browser* riporta la URL della pagina a cui si è collegati nella barra in alto.

La URL riportata come esempio nella figura precedente è:

`https://www.fi.infn.it/index.php/it/`

Spesso alcuni *browser* nascondono la parte iniziale (il protocollo, vedi dopo) per cui viene visualizzata solo una parte della URL. Sempre riferendosi all'esempio in figura, alcuni *browser* possono infatti riportare solo

`www.fi.infn.it/index.php/it/`

ma, facendo *click* con il pulsante sinistro del *mouse* sull'indirizzo, viene visualizzata la URL completa.

Una URL è composta da diverse parti che forniscono informazioni specifiche sull'indirizzo della risorsa.

1. Protocollo

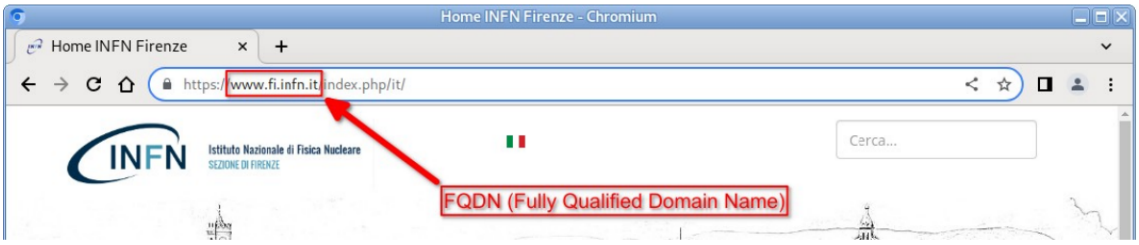
Indica il protocollo di comunicazione utilizzato per accedere alla risorsa, per esempio `http`, `https`, `ftp`, ...

- **`http://`** indica l'utilizzo del protocollo HTTP che permette di accedere a qualsiasi risorsa su Internet attraverso una comunicazione non cifrata: quando ci colleghiamo ad un sito o ad una piattaforma *web* la cui URL inizia con `http://`, dobbiamo tener presente che eventuali malintenzionati presenti sulla rete possono spiare tutto quello che visualizziamo e cosa inseriamo nelle maschere a cui accediamo. Per questo **non dobbiamo mai inserire credenziali o dati particolari in maschere web o piattaforme la cui URL inizia con `http://`**.
- **`https://`** indica l'utilizzo del protocollo HTTPS cioè la versione "sicura" di HTTP: quando ci colleghiamo ad un sito o ad una piattaforma web la cui URL inizia con `https://` e non riceviamo nessun avvertimento dal *web browser* che il sito presenta un certificato non valido, possiamo esser sicuri che la comunicazione è criptata e che il dominio del server (vedi punto successivo) è valido, quindi che eventuali malintenzionati presenti sulla rete non possono spiare né quello che visualizziamo né cosa inseriamo nelle maschere a cui accediamo. Condizione necessaria, ma non sufficiente, per poter inserire le proprie credenziali in una maschera web è

  1. che la sua URL inizi con **`https://`**,
  2. che il *web browser* non segnali problemi col certificato della pagina.

  Per poter essere sicuri di poter inserire le proprie credenzali in una pagina *web* oltre alle precedenti due condizioni deve esser verificato anche il nome di dominio del *server* che ci offre la pagina *web* in questione (vedi punto successivo).

2. FQDN (Fully Qualified Domain Name)



FQDN è l'acronimo di *Fully Qualified Domain Name*, che in italiano significa "nome di dominio completamente qualificato" ed è composto da due parti: il **nome host** e il **nome di dominio**.

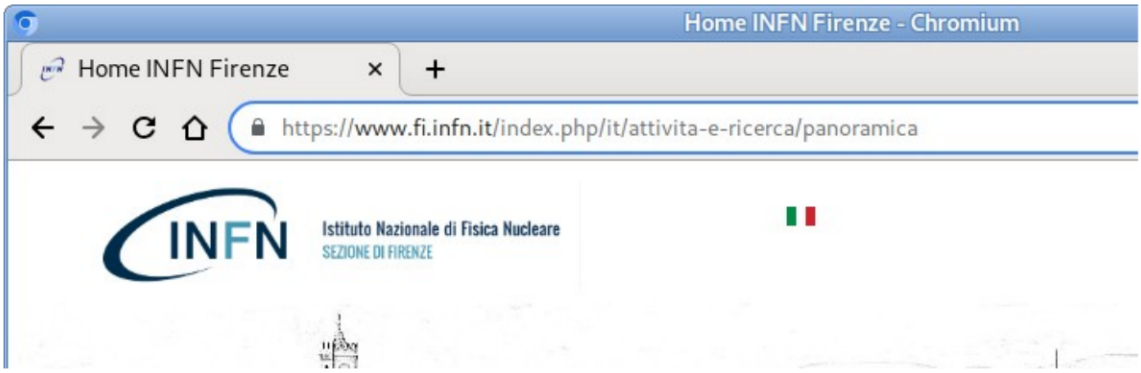
Il **nome di dominio** rappresenta l'identificatore univoco di una particolare organizzazione o risorsa su Internet, è formato da gruppi di caratteri e numeri raggruppati e separati dal punto (".") e si legge da destra verso sinistra. Più a destra si trova il suffisso di dominio (noto anche come dominio di primo livello) che indica la categoria o l'area di appartenenza del dominio come, ad esempio, ".it" (indica l'Italia), ".eu" (indica l'Unione Europea), ".com" (indica un'organizzazione commerciale), ".org" (indica un organizzazione non commerciale), ".edu," (indica un organizzazione educativa), ecc. Il secondo campo a partire da destra indica l'organizzazione o la risorsa di rete come, ad esempio "infn" (indica l'INFN), "cnr" (indica il CNR), ecc. Ci possono essere poi un certo numero di sottolivelli per indicare dipartimenti settori, gruppi o altro come, ad esempio "fi" (indica la Sezione di Firenze dell'INFN).

Il **nome host** rappresenta l'identificatore del server che eroga un particolare servizio all'interno dell'organizzazione o della risorsa Internet e rappresenta il campo più a sinistra nel FQDN.

3. **Percorso**

Specifica la posizione della risorsa all'interno del server. Può includere nomi di *directory* e nomi di *file* separati da barre oblique ("/").

Nell'esempio riportato nella figura seguente



la URL è:

```
https://www.fi.infn.it/index.php/it/attivita-e-ricerca/panoramica
```

1. Il protocollo è: **`https`**

Si tratta quindi di un collegamento criptato (è presente la "s" dopo "http") in cui malintenzionati non possono spiare nè cosa visualizziamo nè cosa inseriamo in eventuali maschere. Se il browser web non ci segnala problemi con il certificato del server siamo certi che (vedi punto successivo) si tratta di un server appartenente alla Sezione di Firenze ("fi") dell'INFN ("infn") che ha sede in Italia ("it").

2. Il FQDN è: **`www.fi.infn.it`**
    - il nome host è: **`www`**
    - il nome di dominio è: **`fi.infn.it`**

    Si tratta di un server con nome host "www" quindi molto probabilmente si tratta del *server web* istituzionale alla Sezione di Firenze ("fi") dell'INFN ("infn") che ha sede in Italia ("it").
3. Il percorso è: **`/index.php/it/attivita-e-ricerca/panoramica`**

Verificare se viene utilizzato il protocollo **`https`** e riconoscere e saper interpretare correttamente e velocemente il FQDN di una URL, cioè ciò che si trova a destra della prima coppia di barre oblique ("//") e a sinistra della prima barre obliqua singola ("/"), permette di verificare immediatamente la bontà di una risorsa a cui stiamo accedendo tramite un web browser.

In particolare tutti i servizi, i portali e le piattaforme INFN

- avranno sempre protocollo **`https`**,
- avranno sempre un certificato valido (nel caso in cui il *web browser* segnali problemi col certificato non si deve mai accettare di proseguire ma è necessario abbandonare immediatamente il sito o la risorsa *web* a cui siamo collegati),
- avranno sempre nome di dominio che termina con **`.infn.it`** (attenzione che non ci devono essere barre oblique "/" nel nome del dominio).

Le uniche 4 eccezioni[13] rispetto a quanto indicato sopra sono rappresentate da:

1. il portale HR Zucchetti dei cedolini dello stipendio, la cui URL inizierà esattamente con

    `https://saas.hrzucchetti.it/hrpistnazfisnuc/`
2. Microsoft OneDrive/Sharepoint, la cui URL inizierà esattamente con

    `https://istnazfisnucl-my.sharepoint.com/`
3. la versione *on-line* di Microsoft Office365, la cui URL inizierà esattamente con

    `https://www.microsoft365.com`
4. il portale "Cisalpina", la cui URL inizierà esattamente con

    `https://mapweb.cisalpinatours.it/`

Seguono alcuni esempi di risorse di rete INFN in cui sono evidenziati il protocollo **`https`** e il dominio (**`.infn.it`**).

- Server web nazionale.....**`https://www.infn.it/`**`altro/altro/...`
- Portale utente.....**`https://portale.dsi.infn.it/`**`altro/altro/...`
- Autenticazione INFN-AAI.....**`https://idp.infn.it/`**`altro/altro/...`

13 In realtà non si tratta di vere "eccezioni": le 4 piattaforme indicate sono servizi che non sono forniti direttamente dell'INFN ma che l'Ente ha acquistato all'esterno e quindi non sono ospitate su *server* INFN.

- Documentale ALFRESCO.....**https://docs.infn.it/**altro/altro/...
- Repository PANDORA.....**https://pandora.infn.it/**altro/altro/...
- Amministrazione Centrale.....**https://www.ac.infn.it/**altro/altro/...
- Servizi Nazionali.....**https://servizinazionali.infn.it/**altro/altro/...
- Agenda.....**https://agenda.infn.it/**altro/altro/...
- ORACLE.....**https://gestionale.dsi.infn.it/**altro/altro/...
- Reclutamento.....**https://reclutamento.dsi.infn.it/**altro/altro/...
- Libro firma.....**https://librofirma.dsi.infn.it/**altro/altro/...
- E-learning.....**https://elearning.infn.it/**altro/altro/...
- Calendario.....**https://calendar.infn.it/**altro/altro/...

Come si può vedere dagli esempi precedenti e come descritto poco sopra, nell'identificare il nome di dominio, si deve considerare solo ciò che è compreso a destra della prima coppia di barre oblique ("//") e a sinistra della prima barre obliqua singola ("/"). Per esempio le seguenti URL, nelle quali viene evidenziato il dominio, non hanno nome di dominio INFN (`.infn.it`) e quindi propongono servizi truffa nonostante siano presenti sigle o nomi che riguardano l'INFN e utilizzino il protocollo `https` (sarebbe uguale anche con `http`):

- `https://in.fn.it/www.infn.it/altro/altro/...`
- `https://portale.dsi.infn.it.eu/altro/altro/...`
- `https://idp.infn.it.it/altro/altro/...`
- `https://docs.infn-it.eu/altro/altro/...`
- `https://pandora.infn.com/altro/altro/...`
- `https://www.ac.infn.org/altro/altro/...`
- `https://www.lnfn.it/altro/altro/...`
- `https://proprio.qualsiasi.cosa/infn.it/altro/altro/...`
- `https://proprio.qualsiasi.cosa/home.infn.it/altro/altro/...`

Gestione di account e credenziali

Le credenziali di un *account* sono la coppia *username* e *password* relative a quel particolare *account*.

Riguardo all'*account* di posta elettronica, un altro parametro fondamentale è l'indirizzo di posta elettronica (che è diverso dall'*username*); tutti gli *account* di posta elettronica di Sezione hanno il seguente formato, salvo casi particolari legati a situazioni di omonimia:

`nome.cognome@fi.infn.it`

Ciascun utente è responsabile della protezione delle credenziali dei propri *account*.

- Non inserire mai le proprie *password* in nessuna pagina web neppure se si ha l'impressione che la richiesta di inserirle provenga dal Servizio Calcolo e Reti o da altri colleghi dell'INFN.

- L'unica pagina *web* dove è possibile inserire le credenziali dell'*account* INFN-AAI deve avere indirizzo che inizia precisamente con[14]

  `https://idp.infn.it/`

  e non ci devono essere segnalazioni di problemi al certificato della pagina da parte del *web browser*.

- L'unica pagina *web* dove è possibile inserire le credenziali dell'account di posta elettronica deve avere indirizzo precisamente uguale a

  `https://selfservice.fi.infn.it:8452`

  e non ci devono essere segnalazioni di problemi al certificato della pagina da parte del browser web.

- Ciascun utente deve custodire con cura le proprie credenziali ed eventualmente deve conservarle in luogo sicuro a cui deve essere l'unico a potervi accedere. In particolare *non* lasciare le proprie credenziali incustodite in ufficio o in altri luoghi.
- Non scrivere le credenziali su *file* salvati in rete, per esempio, su *google drive*, *dropbox*, *microsoft onedrive*, *whatsapp*, *telegram*, *messanger*, *facebook* o simili.
- Non scrivere le credenziali su *file* salvati su dischi esterni o pennette USB che possono esser lasciate incustodite, dimenticate o perse.
- Non salvare mai le password nel *web browser* (su *firefox*, su *chrome* o altro) ma eventualmente è possibile utilizzare Vault dell'INFN (vedi dopo).
- Ciascun utente non deve mai comunicare le proprie credenziali a nessuno, neppure a colleghi e neppure se sono richieste da colleghi con ruoli di responsabilità o con ruoli di coordinatori o con ruoli dirigenziali.
- Non utilizzare le proprie credenziali in postazioni di lavoro diverse dalla propria, cioè non utilizzare le proprie credenziali su PC di colleghi, parenti, amici, o di altri o addirittura in chioschi o *internet point* perché esistono *malware*, detti *keylogger*, che registrano i tasti che vengono premuti sulla tastiera per rubare le credenziali ed inviarle direttamente a malintenzionati. Nel caso di situazioni particolari in cui si presenti la necessità di usare il PC di un collega, sempre che il PC sia in gestione al Servizio Calcolo e Reti, o una postazione messa a disposizione dalla Sezione (per esempio i PC delle sale riunione), ciascun utente deve assicurarsi di eseguire il *"logout"* da qualsiasi *account* utilizzato: non solo il *logout* dell'utente dalla postazione di lavoro ma da tutti i singoli *account* usati nella sessione di lavoro (tipicamente *account* per accedere a piattaforme o servizi *web*, come l'agenda INFN o il portale utente INFN o la *webmail* o altro ancora).
- Non lasciare la propria postazione di lavoro incustodita senza aver eseguito il *logout* dell'utente o aver azionato il blocco della sessione di lavoro protetta da *password*.
- Nella scelta di una *password* non devono essere utilizzate informazioni legate alla propria vita: anche cambiando qualche lettera, per esempio, in numeri o in caratteri speciali o aggiungendo qualche carattere in più, tali *password* risultano particolarmente facili da essere scovate grazie ad opportuni programmi che utilizzano particolari tecniche, dette di "brute force" (in italiano "a forza bruta"), che permettono di

14 In realtà, alla data di stesura di questa guida, ci sono altre due piattaforme *web* che richiedono l'autenticazione con le credenziali INFN-AAI senza passare dalla pagina di autenticazione `https://idp.infn.it/` e sono:
- la pagina di autenticazione del portale documentale INFN (Alfresco) la cui URL è
  `https://docs.infn.it/share/page/`
- il server del repository GitLab-CE
  `https://baltig.infn.it/users/sign_in`

indovinare le *password* a partire da informazioni note riguardanti l'utente. Quindi non devono essere utilizzate informazioni o parti di informazioni inerenti:

  - il proprio nome o cognome;
  - nomi e cognomi di figli o altri parenti, di animali domestici o di altri;
  - date di nascita di parenti, animali domestici o altri;
  - date di laurea, dottorato, inizio lavoro, matrimonio, anniversari o altro;
  - proprio codice fiscale, di parenti o altri;
  - indirizzo di residenza, di lavoro, di parenti o altri;
  - numeri di telefono propri, o di parenti o altri;
  - marca o targa della propria auto, della propria moto o di altro;
  - titoli di film, canzoni, libri o altro;
  - nome di un esperimento, di personaggi famosi, o altro;
  - qualsiasi altra informazione legata alla propria persona o al proprio lavoro.

- Utilizzare *password* di almeno 12 caratteri (meglio 14) mescolando numeri, lettere minuscole e maiuscole e simboli.
- Utilizzare *password* diverse per *account* diversi ed eventualmente utilizzare il Vault INFN, il servizio di registrazione e gestione delle *password* (vedi dopo).
  - In particolare non usare la *password* della posta elettronica per nessun *account* in cui l'*username* coincide con il proprio indirizzo di posta elettronica o comunque se nell'*account* viene registrato l'indirizzo di posta elettronica o se sia in qualche è modo riconducibile a tale indirizzo.
  - Si consiglia vivamente di usare una *password* specifica per il solo *account* di posta elettronica diversa da quella di tutti gli altri *account*.
  - Si consiglia vivamente di usare una *password* specifica per il solo *account* INFN-AAI diversa da quella di tutti gli altri *account*.

Phishing

La probabilità di portare a buon fine un attacco mirato verso un utente o un gruppo di utenti aumenta all'aumentare della quantità e della qualità delle informazioni disponibili della vittima. Per questo, nell'uso della posta elettronica, si deve prestare particolare attenzione a non dare informazioni sui propri *account* o su dati che potrebbero essere utilizzati per compiere un attacco informatico. In particolare è fondamentale imparare a riconoscere e quindi a trascurare i messaggi di *phishing*.

Con questo termine si indica una tecnica sfruttata dai malintenzionati per ingannare la vittima e convincerla a fornire informazioni personali o dati riguardanti i propri *account* fingendosi una persona affidabile.

Gli utenti devono imparare a riconoscere questa tecnica per evitare di divulgare informazioni utili a malintenzionati che potrebbero sfruttarle per compromettere account o per affinare ed elevare il livello d'attacco.

Purtroppo la qualità di questa tecnica è in continuo miglioramento, viene sempre più adattata alla vittima e quindi, per esempio, si riceve sempre più spesso *e-mail* di *phishing* che riescono ad eludere i filtri anti-*spam* e che si dimostrano particolarmente "dissuadenti" verso gli utenti.

Spesso, prima di inviare *e-mail* di *phishing*, viene svolta una vera e propria ricerca dei dati che più o meno consapevolmente le vittime hanno divulgato in rete o che sono stati carpiti con precedenti campagne di *phishing* in modo da confezionare *e-mail* di *phishing* che si adattano ai destinatari riportando riferimenti a persone conosciute, informazioni di lavoro, il logo dell'Ente o della Sezione, riferimenti ad aziende o servizi che si utilizzano, ecc...

Per questo è opportuno che le potenziali vittime sappiano riconoscere queste *e-mail* ingannevoli non solo dal contenuto o dall'ipotetico mittente ma anche e soprattutto dalla tipologia dei dati richiesti. In altre parole tutte le volte che viene richiesto (o viene richiesto di inserire in una pagina web) un *username*, una *password*, il codice fiscale, l'indirizzo *e-mail* o qualsiasi dato personale, particolare o riservato deve scattare un meccanismo di diffidenza verso quanto richiesto. Nel dubbio è opportuno contattare sempre il mittente della richiesta tramite un altro mezzo senza rispondere a *mail* sospette tramite il semplice "Rispondi" (*"Reply"*) per evitare di rispondere ad un indirizzo truffa.

Gli utenti devono sempre aver presente che nessun gestore di qualsiasi servizio (in particolare i Servizi Calcolo e Reti o le Amministrazioni delle Sezioni INFN) chiederanno mai di fornire credenziali o dati relativi ai servizi che stanno offrendo. In altre parole il Servizio Calcolo e Reti non chiederà mai a nessuno dei suoi utenti di comunicare le credenziali di un qualsiasi *account* che gestisce o di inserirle in nessuna pagina web. Inoltre tali richieste non saranno sicuramente fatte per impedire la chiusura di qualsiasi *account* o in seguito al superamento di qualsiasi limite di utilizzo di un servizio o per ragioni di sicurezza.

In altre parole tutte le volte che, per qualsiasi motivo, ci troviamo in una pagina web che ci chiede di inserire le nostre credenziali di posta elettronica (*username* o indirizzo *e-mail* e *password*) possiamo essere sicuri che si tratta di una pagina malevola e che se inseriamo le nostre credenziali queste ci verranno rubate.

L'unica pagina dove, ovviamente, è lecito inserire le nostre credenziali della posta è la *webmail*, anche se ne sconsigliamo vivamente l'uso (vedi una delle sezioni successive "Accesso alla *webmail*").

Attualmente la URL della *webmail* è esattamente:

```
https://selfservice.fi.infn.it:8452
```

Spam Blacklist

Una *"Spam blacklist"* è una lista di nodi che sono stati utilizzati per spedire *spam*. Ce ne sono di pubbliche e di private, gratuite o a pagamento, generate da organizzazioni più o meno serie e utilizzate diffusamente dai *mail server* per riconoscere mail di *spam*.

Tutti gli utenti devono aver ben presente che un loro errore può compromettere il servizio di posta elettronica di tutta la Sezione o dell'intero Ente.

Infatti se un utente cade incautamente in una trappola di *phishing* e in tal modo permette ad un malintenzionato di carpire le proprie credenziali della posta elettronica, il suo *account e-mail* potrà essere utilizzato per inviare altre *e-mail* di *phishing* o di *spam*. In questo modo in brevissimo tempo iniziano a circolare in rete *e-mail* di *phishing* o di *spam* che provengono dal *server* di posta di Sezione o dell'Ente e, in modo automatico tramite sistemi di autoapprendimento, gli altri gestori di posta elettronica inseriscono i nostri server nell'elenco dei server di posta che inviano *spam* (*Spam Blacklist*).

Una volta che i *server* di posta elettronica sono finiti in una o più *Spam Blacklist* si crea un gravissimo disservizio a tutti gli altri utenti che utilizzano lo stesso server di posta perché tutta la posta che invieranno sarà classificata come *spam* e automaticamente respinta.

Un'altra considerazione da tener presente è che non è del tutto banale e scontato ottenere la rimozione del proprio *server* di posta da una *Spam Blacklist*: spesso non c'è la possibilità di interagire con un interlocutore perché

solitamente la gestione di queste liste è automatizzata da processi di autoapprendimento (“Intelligenza Artificiale”, *“Machine Learning”*, ...). In altri casi è necessario addirittura pagare il servizio di cancellazione da una *Spam Blacklist*.

In definitiva un errore di un singolo utente che cade in una trappola di *phishing* ha come conseguenza la compromissione di tutto il servizio di posta elettronica di un’intera Sezione o di tutto l’Ente il cui ripristino risulta particolarmente complicato e con notevole spreco di tempo ed energia se non di denaro.

Allegati

Una delle tecniche più diffuse per far far eseguire un codice malevolo agli utenti e quindi compromettere un PC è quella di allegare un *malware* ad una *mail*.

È quindi di fondamentale importanza disabilitare l’anteprima degli allegati per evitare il rischio di poter mandare in esecuzione un eventuale codice malevolo con la semplice visualizzazione dei messaggi di posta ed aprire gli allegati di una *mail* solo se si è assolutamente certi della loro bontà.

Il fatto che in tutti i server di posta delle Sezioni e dell’Ente siano presenti dei filtri anti-*malware* non implica che l’utente sia automaticamente protetto e che non debba prestare attenzione nell’aprire gli allegati. Tali filtri infatti, anche se riescono a bloccare la maggior parte dei *malware*, non sono infallibili.

In rete sono presenti servizi gratuiti utilizzabili per testare gli allegati. Uno di questi servizi è offerto dal sito

https://virustotal.com/

che permette di caricare un *file* per eseguirne la scansione con decine di anti-*malware*. Per poter utilizzare questi servizi si deve salvare l’allegato sul proprio PC e successivamente caricare il *file* sul sito sopra citato. Questa procedura ha due grossi inconvenienti: per prima cosa si salva sul proprio PC un *file* potenzialmente pericoloso quindi deve essere trattato con estrema cautela ed inoltre, caricando il *file* sospetto su un sito in rete, si possono esporre dati particolari o riservati che potrebbero esser contenuti in tale *file*. Per questo si consiglia di utilizzare questi strumenti solo se si ha completa consapevolezza e padronanza delle operazioni che si stanno effettuando.

Nel dubbio, prima di provare ad interagire con allegati sospetti e potenzialmente pericolosi, si consiglia di contattare sempre il Servizio Calcolo e Reti seguendo la procedura riportata nella guida

https://www-servcal.fi.infn.it:444/doc/miniguida-come_inoltrare_i_messaggi_a_servcal-mail_pericolose_o_di_phishing.pdf

Link

Anche seguire collegamenti (*“link”*) presenti in messaggi di posta o in documenti che ci collegano a contenuti ignoti è particolarmente pericoloso. Infatti l’apertura di un *link* può portare ad una pagina *web* o ad un *file* presente in rete che può contenere un *malware*.

Il collegamento è costituito da due elementi:

- quello che viene visualizzato dall’utente (di solito con un colore dei caratteri diverso dal testo circostante);
- l’indirizzo URL a cui punta il collegamento (vedi una delle sezioni precedenti, “URL”).

Per avere un’indicazione di quale sia la reale destinazione di un *link*, cioè l’indirizzo (URL) a cui punta il collegamento, è possibile muovere il puntatore del *mouse* sopra al *link* stesso e aspettare prima di fare *click* per visualizzare in anteprima la destinazione. L’indirizzo compare di solito in sovrimpressione o nella barra di stato di solito posizionata in basso nella finestra del programma che si sta utilizzando. Questa funzionalità di solito è comunemente abilitata ma eventualmente può essere necessario attivarla nelle preferenze cercando la voce *“tooltip”*. In questo modo possiamo sapere dove punta un indirizzo Internet senza doverlo visualizzare e di volta in

volta è possibile valutare la bontà della destinazione in base a quanto descritto in una delle sezioni precedente ("URL").

È importante non seguire mai *link* presenti nelle *mail* o in documenti a meno che non ci sia l'assoluta certezza della bontà della pagina *web* a cui punta il *link*.

Seguendo un *link* è importante non aprire mai pagine che presentano un certificato non valido: questa situazione viene segnalata dal *web browser* e, in tal caso, è necessario abbandonare immediatamente la navigazione.

Valutare di volta in volta la bontà del *link* che si sta per seguire è di fondamentale importanza, giudicando la corrispondenza fra quanto indicato dal testo del collegamento e l'indirizzo vero e proprio. Per esempio se ci si aspetta di seguire un collegamento verso un contenuto ospitato da un ente di ricerca in Francia ci si deve aspettare un link del tipo "[qualcosa].[qualcosa]. [...].[sigla dell'ente].fr".

È opportuno valutare anche il livello di sicurezza richiesto dal collegamento in base al contenuto. Per esempio se si deve visualizzare semplicemente delle immagini o informazioni generiche ci possiamo aspettare di trovare un indirizzo URL che inizia con "`http:`". Al contrario se ci colleghiamo ad una pagina che contiene dati sensibili (banche, strumenti di pagamento, dati personali, ...) o maschere dove inserire credenziali è necessario, che l'indirizzo inizi con "`https:`".

La pressione psicologica trasmessa alla potenziale vittima dal messaggio che invita a seguire un collegamento rappresenta un'utile arma in mano a malintenzionati: la presenza nel testo del messaggio di aspetti di pressante necessità e di emergenza devono segnalarci una potenziale situazione di pericolo di un collegamento e quindi consigliarci maggiore diffidenza nel seguire quanto proposto.

Se i *link* presenti in un'*e-mail* puntano ad indirizzi non riconducibili al contenuto della *mail* stessa è un'ulteriore indicazione della sua falsità.

Quando si valuta la bontà di un collegamento è necessario prestare particolare attenzione ai caratteri che costituiscono l'indirizzo che siamo invitati a seguire. L'uso di caratteri simili o di sequenze di caratteri simili o simboli o di caratteri di altre lingue (greco, cirillico, ...) che assomigliano a lettere dell'alfabeto che siamo abituati ad utilizzare possono indirizzarci verso destinazioni inaspettate. Ad esempio:

- "`lt`" invece di "`it`" ("`www.infn.lt`" invece di "`www.infn.it`");
- "`rn`" invece di "`m`" ("`www.rni.infn.it`" invece di "`www.mi.infn.it`";
- "`ç`" invece di "`c`";
- "α" invece di "a";
- "×" invece di "x";
- … .

In rete sono presenti servizi gratuiti utilizzabili per testare gli indirizzi (URL) a cui puntano eventuali collegamenti presenti nei messaggi di posta elettronica. Uno di questi servizi è offerto dal sito

`https://virustotal.com`

che permette di verificare se un certo indirizzo punta a del codice pericoloso. Anche in questo caso si consiglia di utilizzare questo strumento solo se si ha completa consapevolezza e padronanza delle operazioni che devono esser effettuate.

Nel dubbio si consiglia di contattare sempre il Servizio Calcolo e Reti prima di seguire collegamenti sospetti. Se il link è contenuto in una mail, inviare tale mail al Servizio Calcolo e Reti seguendo la procedura riportata nella guida

https://www-servcal.fi.infn.it:444/doc/miniguida-come_inoltrare_i_messaggi_a_servcal-mail_pericolose_o_di_phishing.pdf

Link brevi (abbreviazione degli URL)

L'abbreviazione degli URL o abbreviazione degli indirizzi web (in inglese: URL *shortening*) è una tecnica utilizzata per abbreviare lunghi indirizzi *web* (URL) in *link* di pochi caratteri in modo che, per esempio, ne sia più semplice la digitazione.

L'uso di *link* brevi oscura il reale indirizzo di destinazione e può essere utilizzato da malintenzionati per dirigere l'ignaro utente verso un sito o un contenuto pericoloso.

In un messaggio di posta elettronica e in generale nei documenti, la presenza di *link* brevi può essere un'indicazione di qualcosa di malevolo in quanto nell'*e-mail* o nei documenti di lavoro non c'è di solito necessità del loro utilizzo.

Pagine web truffa

Spesso le mail di *phishing* puntano a pagine *web* con grafica e contenuti uguali in tutto e per tutto alle pagine del server *web* di Sezione o di un servizio di Sezione o di un servizio Nazionale ma che in realtà si trovano su un server malevolo e hanno come fine quello di rubare informazioni o credenziali.

Spesso vengono riprodotte pagine di autenticazione del tutto uguali alle pagine di autenticazione che usiamo per esempio per accedere alla posta elettronica o ai Servizi Nazionali (pagina di autenticazione INFN-AAI).

L'utente che non presta attenzione al reale indirizzo (URL) della pagina che si sta consultando e si lascia ingannare solo dall'aspetto grafico della pagina può inserire le proprie credenziali, convinto di accedere al proprio *account* di posta o al proprio *account* INFN-AAI, e in questo modo comunicarle ai malintenzionati che hanno organizzato il *phishing*.

Ripetiamo nuovamente che

- l'unica pagina *web* dove è possibile inserire le credenziali dell'*account* INFN-AAI deve avere indirizzo che inizia precisamente con[15]

  `https://idp.infn.it/`

  e non ci devono essere segnalazioni di problemi al certificato della pagina da parte del *web browser*.

- l'unica pagina *web* dove è possibile inserire le credenziali dell'account di posta elettronica deve avere indirizzo precisamente uguale a

  `https://selfservice.fi.infn.it:8452`

  e non ci devono essere segnalazioni di problemi al certificato della pagina da parte del *web browser*.

Se per esempio vengono inserite le credenziali del proprio *account* di posta in pagine di *phishing*, nel caso più fortunato tale account verrà utilizzato per inviare mail di *spam* con *phishing* mirato o *malware* contribuendo pesantemente ad innalzare il livello di pericolosità dell'attacco e aumentando la possibilità che tale attacco abbia gravi ripercussioni sulla Sezione o sull'intero Ente. Contemporaneamente il server di posta della Sezione o dell'Ente inizia a comparire nelle *Spam Blacklist* e tutti gli altri utenti (di Sezione o dell'intero Ente) non riescono più ad inviare *mail* perché vengono classificate come *spam*. Nel caso meno fortunato, in cui la pagina di *phishing*, sia stata creata da malintenzionati con lo scopo di effettuare truffe, la vittima è esposta alla possibilità di trovare

15 In realtà, come già indicato in una nota precedente, alla data di stesura di questa guida, ci sono altre due piattaforme *web* che richiedono l'autenticazione con le credenziali INFN-AAI senza passare dalla pagina di autenticazione `https://idp.infn.it/` e sono:
- la pagina di autenticazione del portale documentale INFN la cui URL è
  `https://docs.infn.it/share/page/`
- il server del repository GitLab-CE
  `https://baltig.infn.it/users/sign_in`

mail fasulle nel proprio *mail client* che chiedono di fare pagamenti o altre azioni senza avere nessuna possibilità di rendersi conto[16] che sono mail fasulle (vedi sezione "Schema ricorrente di truffe o di attacchi alle Amministrazioni").

Se invece sono state comunicate le credenziali INFN-AAI, i malintenzionati potranno accedere a tutti i dati di lavoro e potenzialmente a tutti gli strumenti lavorativi a cui può accedere l'utente. In questo modo possono esser divulgati dati particolari o riservati esponendo l'Ente a gravissimi danni, a denunce e sanzioni oppure, sfruttando i servizi a cui può accedere l'utente, possono esser intraprese vere e proprie truffe o altre attività illegali.

Webmail

Per facilitare l'uso della posta elettronica viene normalmente messa a disposizione degli utenti un'interfaccia *web* ("*webmail*") attraverso la quale è possibile accedere al proprio account di posta elettronica e leggere, inviare ed organizzare l'*e-mail*.

In questo modo in una qualsiasi postazione dotata di collegamento ad Internet (il proprio PC, tablet o smartphone o quelli di un collega, una postazione di lavoro condivisa, un Internet Point, ...) tramite un qualsiasi browser web (Mozilla Firefox, Google Chrome, Safary, Microsoft Internet Explorer, Microsoft Edge, ...) si è in grado di utilizzare la propria posta elettronica.

Il fatto che esista questa modalità di accesso alla posta non significa che vada usata: come detto in precedenza, accedere alla propria posta elettronica da un PC che non gestiamo in prima persona o che non è gestito dal Servizio Calcolo e Reti è la cosa peggiore che possiamo fare in termini di sicurezza. Non si può essere sicuri che su tali PC non sia presente un *keylogger* che, registrano i tasti che vengono premuti sulla tastiera, ruba le credenziali della posta elettronica e le invia direttamente a malintenzionati e truffatori. Per questo **è assolutamente vietato utilizzare la *webmail* in postazioni di lavoro che non gestiamo in prima persona o che non sono gestite dal Servizio Calcolo e Reti: PC, *tablet* o *smart-phone* di colleghi, parenti, amici, o di altri o addirittura chioschi o *internet point***.

Oltre ai gravi problemi appena esposti, la *webmail* comporta altri rischi di sicurezza in più rispetto all'uso di agenti di posta (*"mail client"*) anche se viene utilizzata nella propria postazione di lavoro.

Infatti nei *mail client* la configurazione di connessione al server di posta elettronica viene fatta una volta per sempre quindi l'utente non deve prestare attenzione e non deve preoccuparsi dell'autenticità del collegamento tutte le volte che legge un messaggio o che scarica la posta.

Usando la *webmail* invece si deve verificare l'autenticità del *server web* tutte le volte che ci colleghiamo e quindi verificare che si tratti di un collegamento che punta ad un indirizzo che inizia con "`https://`", che il nome del *server web* sia quello della Sezione (`https://selfservice.fi.infn.it:8452`) o dell'Ente e che il certificato elettronico del *server* sia valido. Se non vengono compiute queste tre verifiche tutte le volte, l'utente rischia di inserire le proprie credenziali in un *server* fasullo e in tal modo di compromettere il proprio *account* di posta.

Per tutto quanto detto sopra si consiglia vivamente di non usare giornalmente la *webmail*; meglio ancora se non viene proprio mai utilizzata in particolare da utenti afferenti ai Servizi di Amministrazione, Servizi di Direzione, Servizio Tecnico, Servizio Calcolo e Reti, dai RUP e da chi ha ruoli dirigenziali, di coordinamento e di gestione di fondi.

16 L'impossibilità della vittima di rendersi conto che queste mail sono fasulle non deriva da inesperienza, leggerezza nel leggere la mail o disattenzione: anche un esperto non potrebbe rendersi conto che tale mail è creata in modo fraudolento; solo confrontando il contenuto degli *header* (vedi dopo per una definizione) della *mail* con i dati contenuti nei file di *log* del *mail server* si potrebbe verificare l'origine criminale.

Account privati

Sebbene il disciplinare INFN permetta l'uso di strumenti informatici dell'Ente anche a fini personali, purché non abbia una ricaduta sull'attività lavorativa o sull'Ente stesso, si consiglia di utilizzare il proprio *account* di posta elettronica istituzionale (`...@fi.infn.it`) solo a scopi lavorativi e mantenere separate le *e-mail* personali da quelle di lavoro in modo che sia più semplice riconoscere *e-mail* fasulle e ridurre il rischio di credere ad *e-mail* di *phishing*: così facendo sarà ovvio all'utente che eventuali messaggi arrivati al proprio *account* di posta di lavoro e provenienti da siti di acquisti *on-line*, banche, poste, carte di credito sono ovviamente fasulli.

In altre parole, attivando un *account* di posta elettronica privato diverso da quello di lavoro ed usandolo per la propria vita personale, nel caso arrivi nell'*account* di lavoro una *mail* relativa alla propria vita privata come l'avviso di un acquisto in consegna, una fattura di luce, gas, telefono da pagare, una vincita ad una lotteria (a cui non avete comunque mai partecipato), una richiesta di aiuto da un parente lontano, ecc. sapete con certezza che si tratta di una *mail* falsa.

I moderni agenti di posta elettronica per PC, *tablet* e *smartphone* permettono di gestire simultaneamente più *account e-mail* quindi possiamo gestire sia l'*account* di lavoro che quelli personali con lo stesso strumento in modo semplice sulla stessa postazione di lavoro mantenendo separati i due ambiti.

Intestazioni dei messaggi di posta

Un messaggio di posta elettronica è costituito da due parti:

- l'intestazione (*"header"*) che contiene alcune informazioni del messaggio come il mittente, il destinatario, l'oggetto , data e orario d'invio dell'*e-mail* ed altre informazioni relative alla storia dell'*e-mail* come ad esempio i nomi dei *server* di posta che hanno gestito la consegna, eventuali annotazioni da parte dei filtri ed altro ancora;
- il corpo del messaggio (*"body"*) cioè il contenuto vero e proprio del messaggio (inclusi gli allegati).

Di solito in un *client* di posta elettronica viene visualizzato il mittente, il destinatario e la data di spedizione mentre tutte le altre informazioni presenti nell'*header* rimangono nascoste. Per visualizzare tutti i dati contenuti nell'h*eader* è necessario accedere al sorgente (*"source"*) del messaggio. Per esempio, in Mozilla Thunderbird, una volta evidenziato il messaggio si può accedervi premendo i tasti "`Ctrl + U`" oppure, dalla barra dei menu, "Visualizza" > "Sorgente del messaggio".

Sebbene praticamente tutti i dati presenti nel messaggio di posta possono essere falsificati (mittente, primi server di spedizione del messaggio, date, contenuti, ...) le informazioni contenute nelle intestazioni (*header*) possono dare varie informazioni che possono essere di aiuto per valutare se un messaggio è fasullo.

Però l'interpretazione degli *header* dei messaggi non è banale e riguarda più gli addetti ai lavori che non gli utenti di posta.

In caso di dubbi sulla bontà di un messaggio di posta si consiglia di inoltrare tale messaggio al Servizio Calcolo e Reti: seguendo la procedura riportata nella guida

https://www-servcal.fi.infn.it:444/doc/miniguida-come_inoltrare_i_messaggi_a_servcal-mail_pericolose_o_di_phishing.pdf

che permette di inoltrare il contenuto completo della mail (intestazione + corpo del messaggio) altrimenti con un semplice inoltro del messaggio viene inviato solo il corpo del messaggio e quindi mancherebbero informazioni fondamentali per una corretta analisi.

Vault INFN: servizio di gestione delle password

Il sistema consente ad un utente INFN la gestione delle proprie credenziali tramite il *software open source* Vaultwarden (https://github.com/dani-garcia/vaultwarden), un fork del password manager bitwarden.

Il servizio è fornito dai Servizi Nazionali INFN tramite server interni alla rete INFN (servizio *self-hosted*) gestiti da personale INFN.

Le *password* che gli utenti gestiscono tramite questo servizio non vengono salvate in chiaro sui server INFN ma sono criptate tramite una *password* principale (*"master password"*) di cui solo l'utente è a conoscenza. Questo comporta che

- i colleghi che gestiscono il server non possono vedere le *password* degli utenti;
- se l'utente perde la *master password*, tutte le *password* salvate risulteranno inaccessibili e neppure i colleghi che gestiscono il server potranno ripristinarle.

L'utente accede al servizio all'indirizzo del server https://vault.infn.it autenticandosi con le proprie credenziali INFN-AAI (diverse dalla *master password*).

Il Servizio Calcolo e Reti della Sezione non ha nessun permesso di gestione degli *account* Vault ma mette a disposizione la seguente guida per la richiesta del servizio, l'installazione e la configurazione:

https://www-servcal.fi.infn.it:444/miniguide/miniguida-vaultwarden-gestore_di_password.pdf

Posta elettronica: come difendersi

Purtroppo, come indicato nell'introduzione di questa guida, non esiste una ricetta standard da applicare indistintamente a tutte le situazioni che si possono presentare e a tutti i messaggi di *e-mail* che riceviamo per essere certi di esser al riparo da tutti i problemi di sicurezza.

Solo con un atteggiamento ed un comportamento di consapevole responsabilità nell'utilizzo della rete e della posta elettronica possiamo essere sufficientemente tranquilli di non intraprendere azioni che possono avere gravissime conseguenze per noi stessi e per l'Ente.

Oltre alle raccomandazioni riportate sopra, ed in particolare nelle sezioni

- **Gestione di account e credenziali,**
- **Phishing,**
- **Allegati,**
- **Link,**
- **Account privati,**

per quanto riguarda la posta elettronica, si consiglia di seguire le seguenti indicazioni.

1. Non si deve assolutamente sottovalutare né il valore dei dati contenuti nei PC di lavoro, di quelli a cui accediamo tramite i nostri *account* e di quelli presenti nei messaggi di posta elettronica né le conseguenze disastrose che possono derivare da un uso incauto dei propri *account* (in particolare quello di posta elettronica) o dalla diffusione o dal furto delle nostre *credenziali*.
2. **Ripetiamo di nuovo la cosa più importante. Se non si custodiscono con cura le credenziali del proprio *account* di posta elettronica, si comunicano ad altre persone o, cadendo in un *phishing*, si inseriscono in una pagina *web* di truffa si espone completamente il proprio *account* di posta a malintenzionati e**

truffatori che possono depositarvi qualsiasi *mail* con qualsiasi contenuto; non è possibile identificare in nessun modo tali *mail* come malevole. In questo modo può essere richiesto di compiere qualsiasi azione da un superiore, da un collega o da altri, per esempio, può essere chiesto da parte di un falso fornitore, che comunque la vittima identifica come reale, di fare un pagamento su un conto appositamente creato per una truffa. Oppure il proprio account può essere usato per inviare *mail* con richieste o contenuti falsi a colleghi, fornitori, parenti, amici o altri che, ovviamente, considereranno tali *mail* come autentiche.

3. Si deve avere almeno una minima conoscenza degli strumenti che si utilizzano giornalmente al lavoro:
   - sapere cosa sia un *web browser*;
   - sapere cosa sia un agente di posta elettronica (o *mail client*);
   - sapere cosa si intende per *webmail*;
   - sapere cosa sia un collegamento (o *link*) e una URL;
   - sapere, in un *web browser*, dove viene visualizzato o inserito l'indirizzo URL di una pagina *web* che si sta consultando o che si intende visualizzare;
   - sapere come visualizzare le informazioni relative al certificato digitale di una pagina *web* che si sta consultando.
4. Si deve sempre aver presente che (per la natura del meccanismo di scambio di *e-mail*) praticamente tutti i dati presenti nel messaggio di posta possono essere falsificati (mittente, primi *server* di spedizione del messaggio, date, contenuti, ...). In particolare, a meno che il messaggio non sia firmato digitalmente, non c'è nessuna sicurezza sull'identità del mittente.
5. Si deve sempre aver presente che, sempre per la natura del meccanismo di scambio di *e-mail*, i messaggi di posta viaggiano in chiaro su Internet quindi non dovranno mai contenere credenziali o dati particolari perché eventuali malintenzionati in agguato in rete potrebbero carpire tali informazioni.
6. Quando nel testo dei messaggi di posta è presente un *link* che rimanda alla *webmail* (o più probabilmente ad una pagina *web* opportunamente realizzata in modo da risultare uguale alla pagina di autenticazione della *webmail*) si può essere praticamente certi che si tratta di un messaggio di *phishing* e si deve immediatamente interrompere il collegamento.
7. Diffidare di messaggi con richieste di informazioni relative ai propri *account* o alle proprie credenziali: nessun amministratore di qualsiasi servizio vi chiederà mai informazioni relative a quel servizio perché già ne è in possesso.
8. Diffidare di messaggi che presentino aspetti di pressante necessità e di emergenza.
9. Diffidare di messaggi che vi informano di problemi di sicurezza nei vostri *account* o la saturazione dello spazio a disposizione della vostra posta elettronica e vi invitano a riempire una maschera in una pagina *web* chiedendovi *username* e *password*.
10. Diffidare di messaggi in cui sono proposti *link* a pagine web. Se ci sono *link* è opportuno esaminarli con grande attenzione, tenendo conto che quello che viene riportato nel messaggio non è necessariamente l'indirizzo che si aprirà nel *web browser*: posizionare quindi il puntatore del mouse sul *link*, e verificare la reale destinazione del collegamento. In particolare verificare che inizi con ''`https://`'' e che sia compatibile con l'indirizzo che ci si aspetta di visualizzare non, ad esempio, `www.paypal.finto.tw` o `www.ebbay.it` (cioè quasi uguale a quello vero), o addirittura numerico. In ogni caso è sempre buona norma non fare *click* sui *link*, ma digitarli direttamente nella barra degli indirizzi (URL) del *web browser*.

Verificare l'indirizzo di destinazione con strumenti di analisi presenti in rete (ad esempio tramite il sito https://virustotal.com). Se tutti i link presenti in un'*e-mail* puntano allo stesso indirizzo o ad indirizzi diversi e non riconducibile al contenuto della *mail* stessa è un'ulteriore indicazione della sua falsità.

11. Diffidare di messaggi in cui sono presenti *link* brevi in cui è oscurato il reale indirizzo di destinazione.
12. Diffidare sempre di richieste di informazioni finanziarie, dati particolari o riservati.
13. Diffidare di messaggi che promettono provvigioni favolose per il trasferimento di eredità o di ingenti quantità di denaro tramite il vostro conto corrente.
14. Diffidare di messaggi in cui un vostro conoscente che vi scrive di trovarsi all'estero, di essere stato derubato e vi prega di spedirgli un po' di soldi per potersi comprare il biglietto di ritorno.
15. Diffidare di messaggi in cui è presente qualsiasi forma di ricatto e, per esempio, vi viene chiesto del denaro per non rivelare a terzi vostre foto, video, comportamenti o altro.
16. Diffidare di messaggi contenenti comunicazioni di vincite, premi, concorsi o lotterie *on-line* (anche solo per il fatto che non avete mai partecipato a concorsi o lotterie *on-line*!).
17. Diffidare di messaggi in cui venite contattati dalle forze dell'ordine in seguito vostri comportamenti illegali: se avete fatto qualcosa di illecito vengono direttamente ad arrestarvi, non vi avvertono via *mail*, e sicuramente non vi chiedono del denaro per evitare una denuncia.
18. Per una verifica più approfondita dei messaggi di posta elettronica, tramite il client di posta elettronica, si può visualizzare il testo "sorgente del messaggio" ed in particolare l'intestazione del messaggio di cui normalmente vengono visualizzate solo i dati più importanti (mittente, destinatario, data di invio,...). Pur tenendo conto che anche i dati contenuti nell'intestazione dei messaggi possono esser contraffatti si possono ricavare alcune indicazioni sulla bontà del messaggio stesso ma l'interpretazione non è banale e richiede conoscenze tecniche specifiche. Se non si è in grado di interpretare tali informazioni è comunque importante considerare che tali informazioni sono presenti solo nel messaggio originale e che vengono perse qualora si inoltri tale messaggio per richiedere un parere al personale tecnico. In altre parole, per permettere una valutazione della bontà di un'e-mail non è sufficiente inoltrare tale email al Servizio Calcolo e Reti: lo si deve fare seguendo la procedura riportata nella guida

https://www-servcal.fi.infn.it:444/doc/miniguida-come_inoltrare_i_messaggi_a_servcal-mail_pericolose_o_di_phishing.pdf

Indice