Assistenza

Tecnico a distanza

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

- E’ in qualche caso opportuno permettere l’accesso remoto alla propria macchina da parte di un tecnico universitario ad esempio per il controllo delle dotazioni di sicurezza di una postazione
- In tal caso attualmente adottiamo il software di assistenza remota TeamViewer

Filmato:

3 assistenza remota

Aprire una chiamata

- Prima di chiamare l'assistenza dicendo che la **rete** non va, assicurarsi che il problema non dipenda da altri fattori:
  - Verificare il proprio indirizzo usando https://myip.units.it
  - Eseguire un test di velocità usando https://speedtest.units.it
  - Mandare, insieme alla richiesta di assistenza, la cattura schermo dei due test precedenti

Controllo connettività

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

- Se da casa non si accede ai due link indicati in precedenza e nemmeno a http://test.eolo.it/, allora con ottima probabilità il problema non è dell'Università di Trieste
- Controllare il proprio impianto ed eventualmente contattare il proprio fornitore di connettività Internet (ISP)

Filmato:

6 Info Connessione e Cattura Schermo

Desktop Remoto

Filmato:

5.1 Collegamento al Desktop Remoto

5.2 Stampa [5] da remoto e trasferimento file

Fine sessione di lavoro

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

- Disconnettere il Desktop Remoto [9]
- Disconnettere la VPN
- Cancellare eventuali file Universitari copiati sul PC di casa (non dovrebbe esser stato necessario copiare alcun file)
- Disconnettere l’utente SmartWork

Sicurezza dei file

CryptoLocker

- Il CryptoLocker è un Malware (Virus) che viene scritto e diffuso in modo da monetizzare il crimine tramite riscatto (ransom).
- Entra quindi a pieno titolo nei software a scopo estorsivo detti RansomWare.

CryptoLocker

- Cripta (codifica) le informazioni accessibili all'utente con una chiave in mano solo all'organizzazione criminale:
  - Disco rigido
  - Chiavette USB o dischi collegati
  - Dischi di rete a cui l'utente ha accesso in scrittura
  - Dati in cloud con accesso effettuato

CryptoLocker

- Solitamente il pagamento viene chiesto tramite criptovaluta (Bitcoin) e non sempre viene poi data la chiave per la decifrazione
- Se si è affetti da un RansomWare bisogna dare per compromessi tutti i dati accessibili all'utente locale

Misure di sicurezza operativa

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

- Scollegare unità di rete, chiavette e sessioni non necessarie
- Usare utenti non amministratori per lavorare
- Evitare di eseguire/aprire/scaricare file sospetti
- Non inserire chiavette USB di origine sconosciuta

CryptoLocker

Payment for private key

Private key will be destroyed on
9/20/2013
6:48 PM

Time left
71 : 57 : 22

Choose a convenient payment method:

Bitcoin (most cheap option)

bitcoin

Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.

You have to send below specified amount to Bitcoin address **1KP72fBmh3XBRfuJDMn53APaqM6iMRspCh** and specify the transaction ID, which will be verified and confirmed.

Home Page
Getting started with Bitcoin

Enter the transaction ID and press «Pay»:

2 BTC

<< Back

PAY

Misure di sicurezza operativa

- Minimizzare (o richiedere di minimizzare) l’accesso in scrittura ai soli dati che effettivamente si utilizzano organizzandoli a tale scopo

Navigazione WEB

Misure di sicurezza operativa

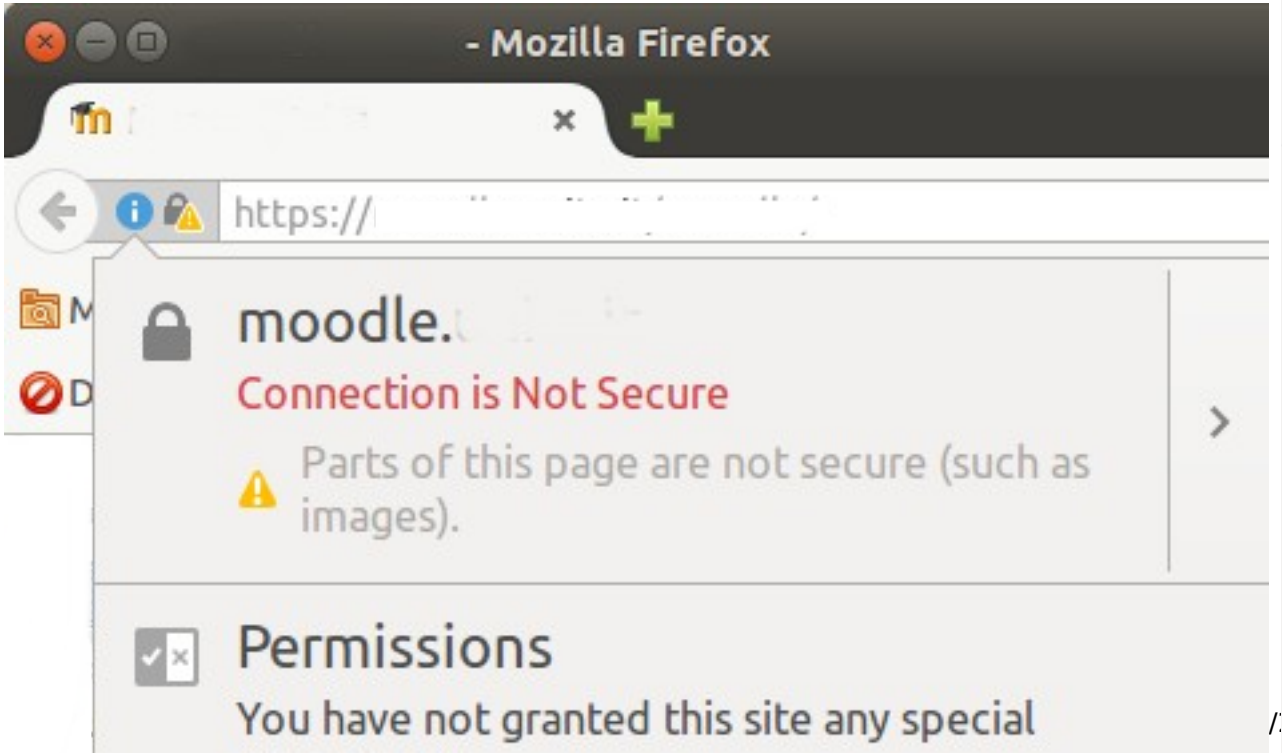
UNIVERSITÀ
DEGLI STUDI DI TRIESTE

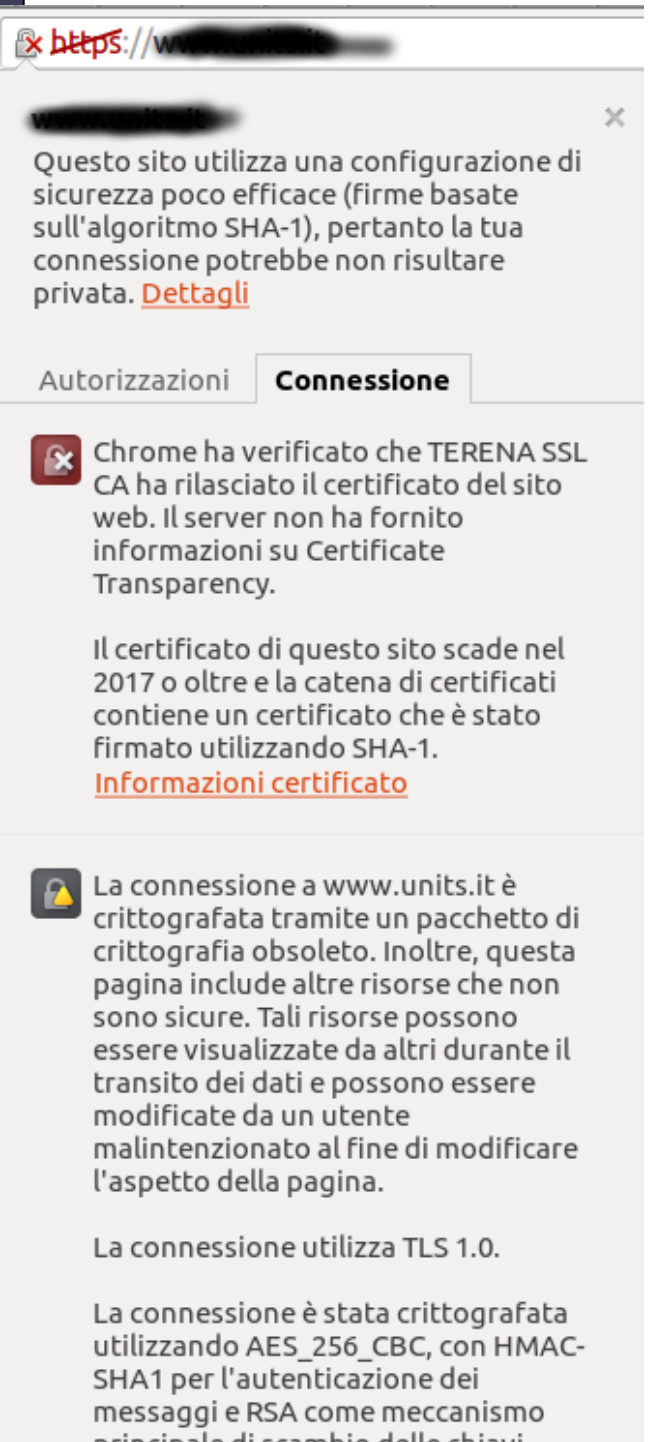
- Verificare dove puntano i collegamenti prima di cliccarci sopra
  - Passando col mouse sui collegamenti, viene sempre visualizzata la destinazione in basso

Certificati

UNIVERSITÀ
DEGLI STUDI DI TRIESTE

- Verificare sempre la sicurezza del sito
- In presenza di warning, se il sito è lavorativo, segnalare





Sicurezza WEB

- Se il lucchetto non è chiuso i nostri dati sono a (più o meno) rischio
  - Dipende dalla sicurezza delle linee che usiamo
- Per i siti istituzionali pretendere da chi è preposto che il lucchetto sia chiuso

Posta Elettronica

Usi impropri

- File da più di 10 MB andrebbero trasferiti con altri mezzi
  - https://filesender.garr.it
- Mail a gruppi di studenti o di dipendenti, liste di iscritti a convegni, ecc… vanno gestiti diversamente tramite mailing lists, liste di distribuzione, newsletter
- Ci sono implicazioni di GDPR se si usano servizi in cloud
  - Chiedere sempre all'Area Servizi ICT

Pericolo allegati

- Allegare documenti alle email è pericoloso perché abitua a cliccare su di essi anche quando la mail potrebbe essere sospetta [4]
- Preferire la scrittura di email solo testo senza html o allegati
  - Nell'html si possono nascondere link malevoli e javascript malevolo

A: CC: CCN: Reply

- CC: Messaggio in copia
- Rispondi a tutti (reply to all) permette di non perdere persone per strada
- CCN/BCC: permette di mettere una persona in copia senza che gli altri lo sappiano

Header falsificabili

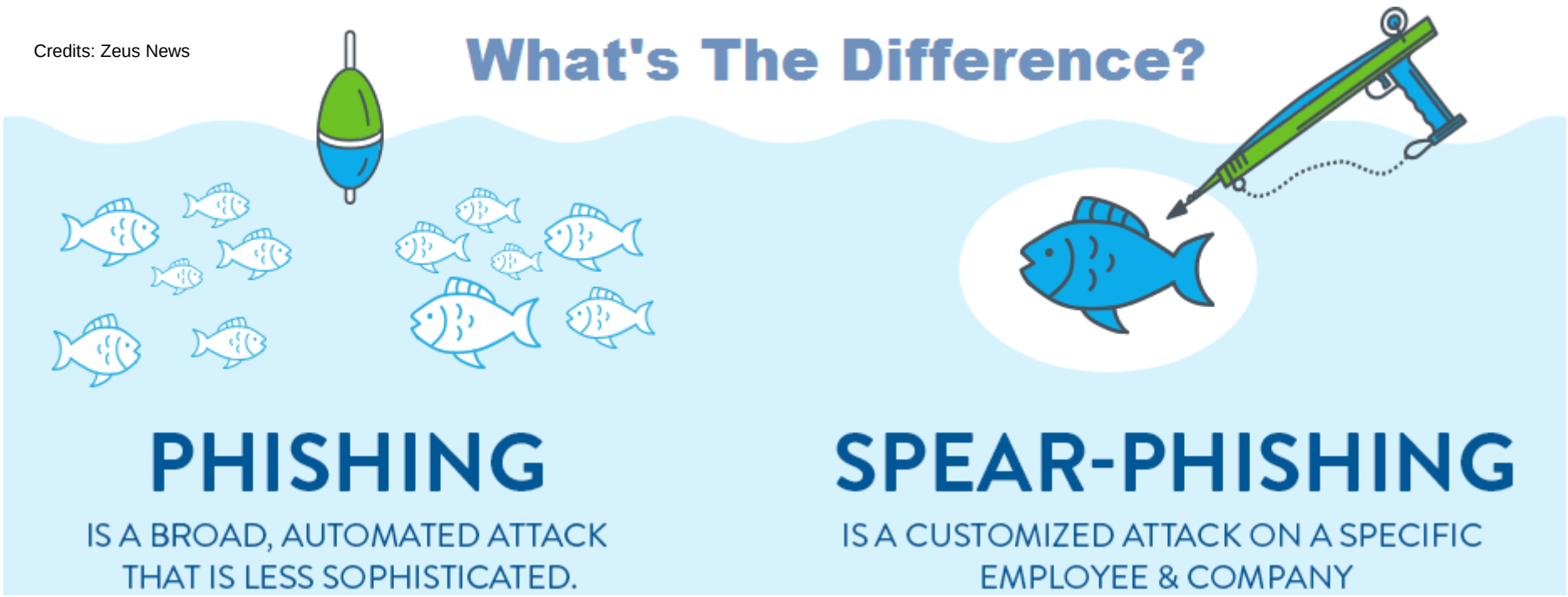
- Mittente e destinatario della posta elettronica sono facilmente falsificabili
- Verificare SEMPRE il flusso documentale per altre vie
  - Prendere gli indirizzi dal phonebook
  - Telefonare
  - Chiedere conferma via sms, whatsapp, ecc…

Phishing

- Phishing è la tecnica di fingersi un mittente lecito e con argomentazioni plausibili carpire informazioni riservate.
- Spear Phishing è un Phishing che è teso a minare la catena di comando di una istituzione agendo su dipendenti specifici
- Accendere il cervello e notare particolari sospetti come: italiano approssimativo, scarsa conoscenza dei contesti, intestazioni sospette.

Phishing

Credits: Zeus News



- Phishing e Spear Phishing si possono combattere con
  - Firma elettronica qualificata (PEC)
  - Firma elettronica

Callback verification

- Un mezzo di verifica valido è la richiamata su indirizzo/telefono non dichiarato
  - Internamente usando il phonebook
  - Esternamente cercando su Internet
- Verificare anche chiamate o email da forze dell'ordine