CONSIGLIO NAZIONALE INGEGNERI

C3i COMITATO ITALIANO INGEGNERIA INFORMAZIONE

Truffe informatiche finanziarie

A cura di Ugo LOPEZ

GdL Cyber Security

Chi sono

- Ingegnere informatico (OIBA) e informatico forense
- Referente commissione terzo settore
- Componente gruppi di lavoro C3i CyberSecurity, Industria 4.0 e Sanità Digitale
- Docente Uniba Informatica Forense e Sicurezza nelle Reti e nei Sistemi Distribuiti
- Autore LinkedIn cloud security

Alcuni tipi di truffe finanziarie

- Schema piramidale/Ponzi (fonte CONSOB)
- Prestazione abusiva di servizi di investimento (fonte CONSOB)
- Clonazione di carte di credito
- **Truffe bancarie**

Phishing

Posteitaliane

Gentile Cliente ,

Abbiamo notato dell'attività insolita nella sua carta
Il suo accesso al portale carte titolari è stato temporaneamente bloccato per la sua tutela

Si prega di confermare la propria identità attraverso il nostro collegamento sicuro

Accedi a collegamento sicuro

Grazie

Per favore, non rispondere a questa e-mail.

Smishing

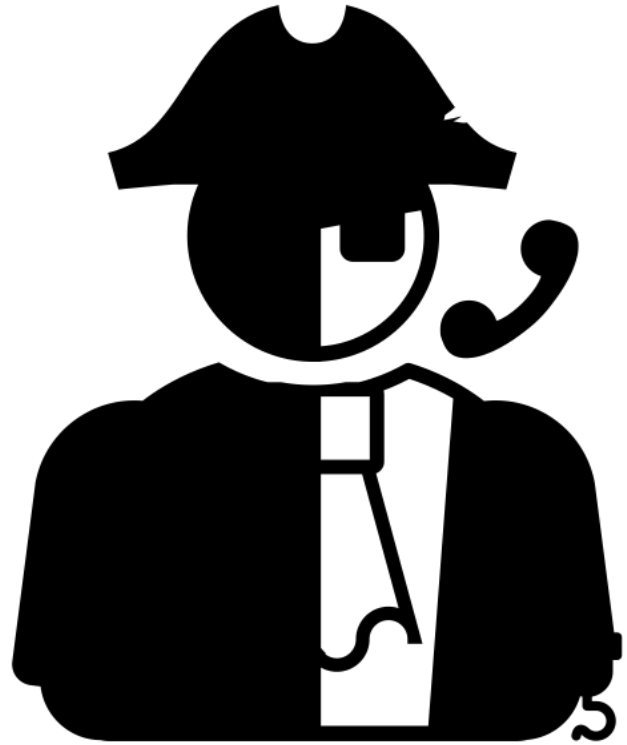
IntesaSP

Tuesday, Nov 17 · 1:57 PM

Gentile cliente, abbiamo rilevato un accesso anomalo al suo conto business segua la procedura per verificare https://is.gd/ilmioprofilo

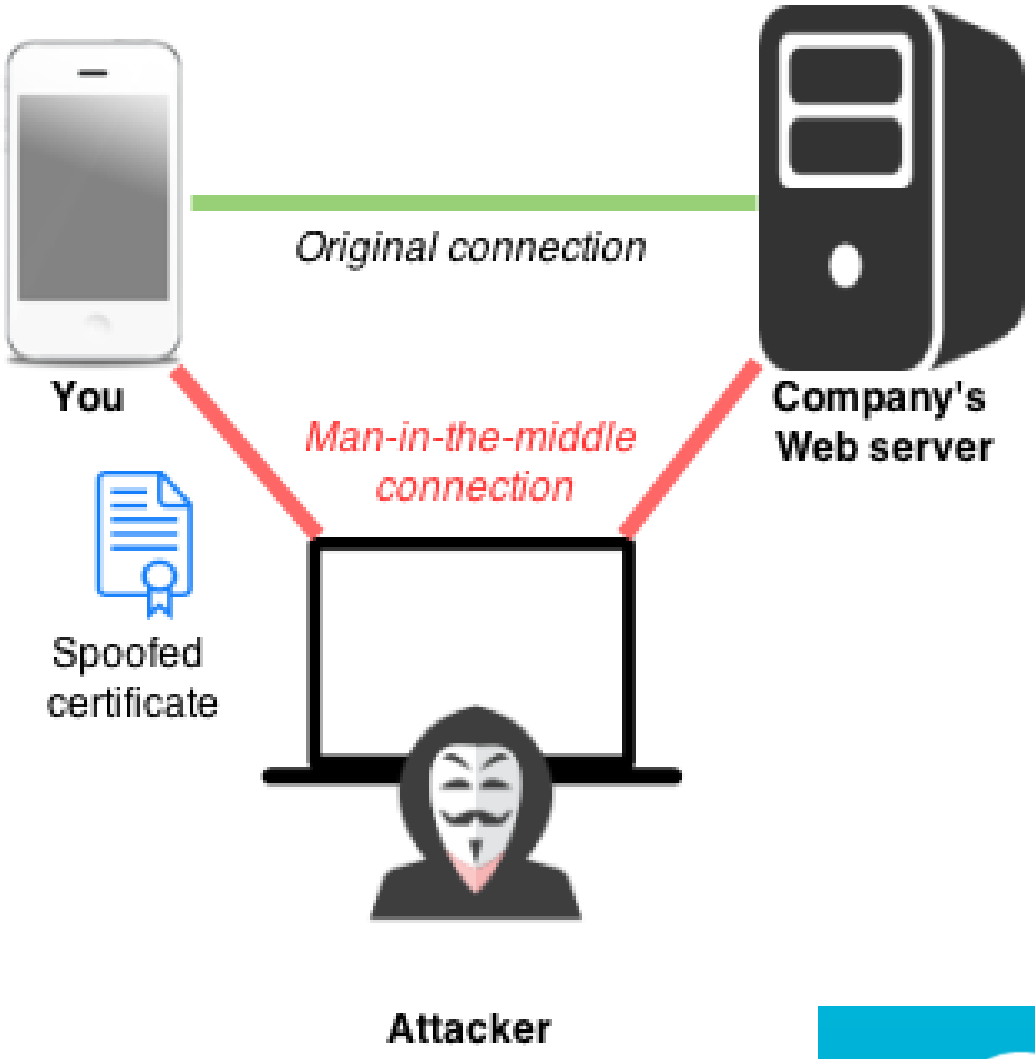
Gentile cliente, abbiamo rilevato un accesso anomalo al suo conto business segua la procedura per verificare https://is.gd/ilmioprofilo

Vishing



Created by Jorge Reyes
from Noun Project

Attacco Man-In-The-Middle



Attacco Mail in the Middle

reF: 346416 Come verifica la password. 16:21:52 12/3/2020

[redacted]

Accountnoninuso noninuso
gio 03/12/2020 15:21

[redacted]

Account Microsoft

Attività di accesso insolita

Abbiamo rilevato attività insolite durante un recente accesso all'account Microsof[redacted]

Dettagli accesso

Paese/area geografica: Italy

Indirizzo IP: 31.171.154.133

Data: 16:21:52-12/3/2020 (GMT)

Piattaforma: Windows

Browser: Chrome

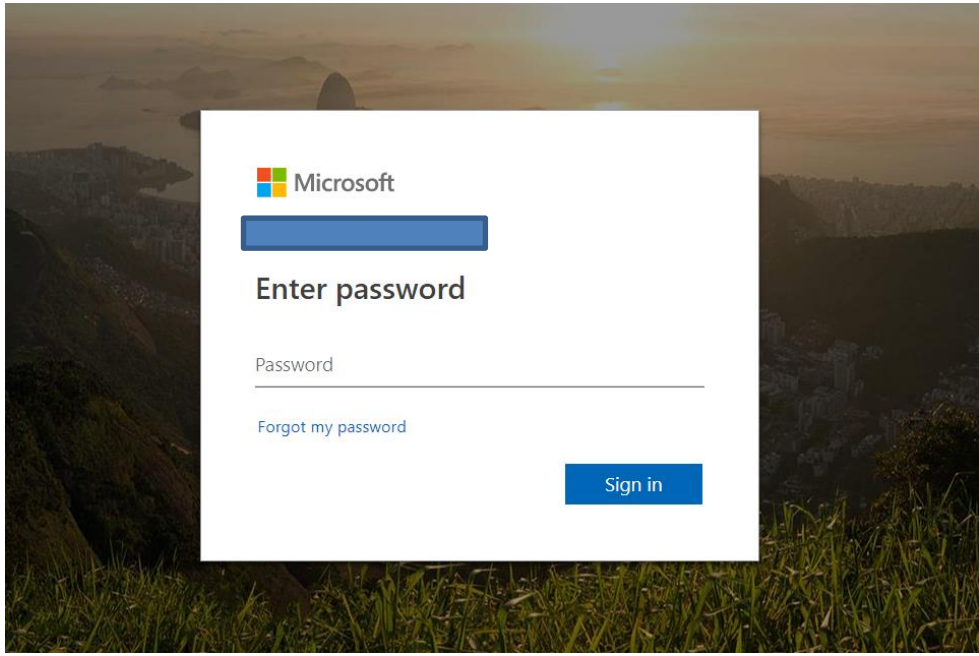
Vai alla pagina delle attività recenti per segnalarci se queste attività sono state eseguite da te. Se non sei stato tu, ti aiuteremo a proteggere l'account. Se sei stato tu, considereremo attendibili attività simili in futuro.

Verifica le attività recenti

Per scegliere di non ricevere le notifiche o modificare la modalità della loro ricezione, fai clic qui.

Grazie,
Il team degli account Microsoft

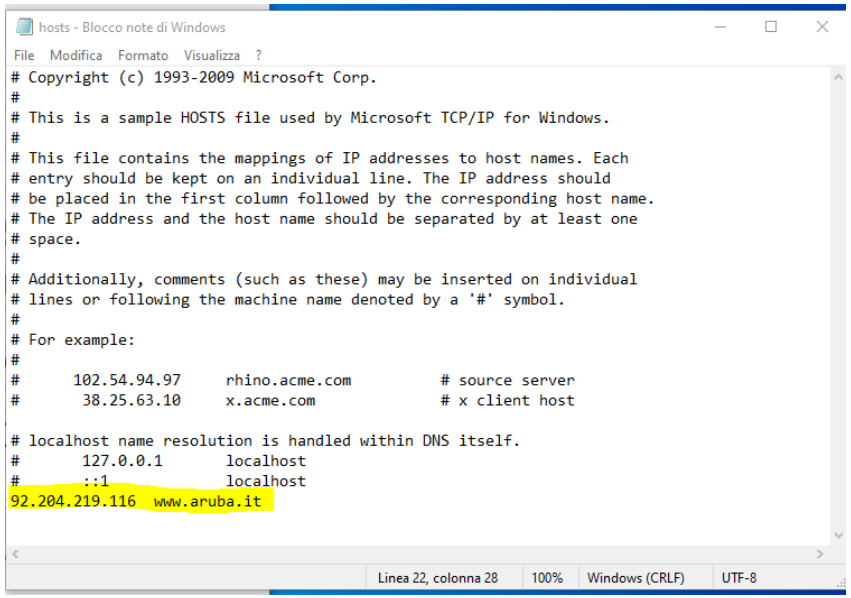
Rispondi | Inoltra



3-137-158-0.cprapid.com/x.php?id=[redacted]

GdL Cyber Security

Hijacking – modifica hosts file



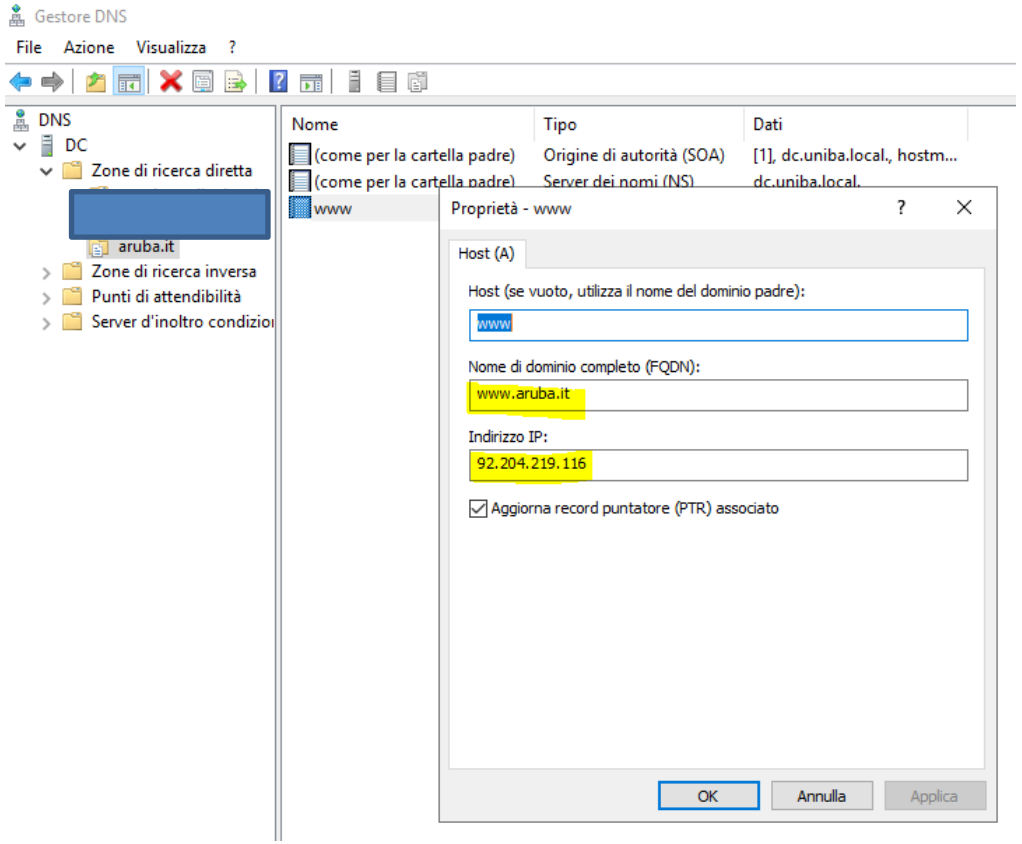
Prima

```
Pinging www.aruba.it [62.149.188.209]
```

Dopo

```
Esecuzione di Ping www.aruba.it [92.204.219.116]
```

Hijacking – DNS Poisoning



Prima

```
Pinging www.aruba.it [62.149.188.209]
```

Dopo

```
Esecuzione di Ping www.aruba.it [92.204.219.116]
```

Code injection

```
<script type="text/javascript">
// <![CDATA[

    Liferay.Util.addInputFocus();          var r=
[redacted]SPA'.split('+').join(' ');
    if (r.length>10){
    var rr=r.split(","), d=[],t='';

    if ($('.data-table-body td').length){
            for (var i=0;i<$('.data-table-body td').length;i++){
                for (var j=0;j<rr.length;j++){
                    try{
                        if (rr[j].length>3){
                            d=rr[j].split(":");
                            if (d[0].length>2){t=$('.data-table-body td:eq('+i+')').html();if(t.indexOf(d[0])>-1){t=t.replace
                            (new RegExp(d[0], 'g'),d[1]);  $('.data-table-body td:eq('+i+')').html(t);}}
                        }
                        $('.data-table-body td:eq('+i+')').attr('style','color:#5f5f65');
                    }catch(easde){}
                }
            }
    }
    }else{$('.data-table-body td').attr('style','color:#5f5f65');}
        Liferay.Portlet.runtimePortletIds = ['menu_WAR_webcontocsupportportlet','sca_WAR_webcontoccommonsportlet',
        'autocensimento_WAR_webcontocusermanagerportlet','footer_WAR_webcontocsupportportlet',
        'breadcrumbs_WAR_webcontocsupportportlet','103','loadcontent_WAR_webcontocutilitiesportlet',
        'monosia_WAR_webcontocutilitiesportlet'];
    // ]]>
</script>
```

Come difendersi (URL)

- Verificare URL (https://unshorten.it/)

Unshorten.It!

https://is.gd/ilmioprofilo

Unshorten.It!

Not got a short URL to try? Here's one: http://bit.ly/GVBQJS

Account Suspended

Destination URL:

https://latuafiliale.com/cgi-sys/suspendedpage.cgi

Description:

Come difendersi (dominio)

- Verificare la proprietà del dominio (https://whois.domaintools.com/)

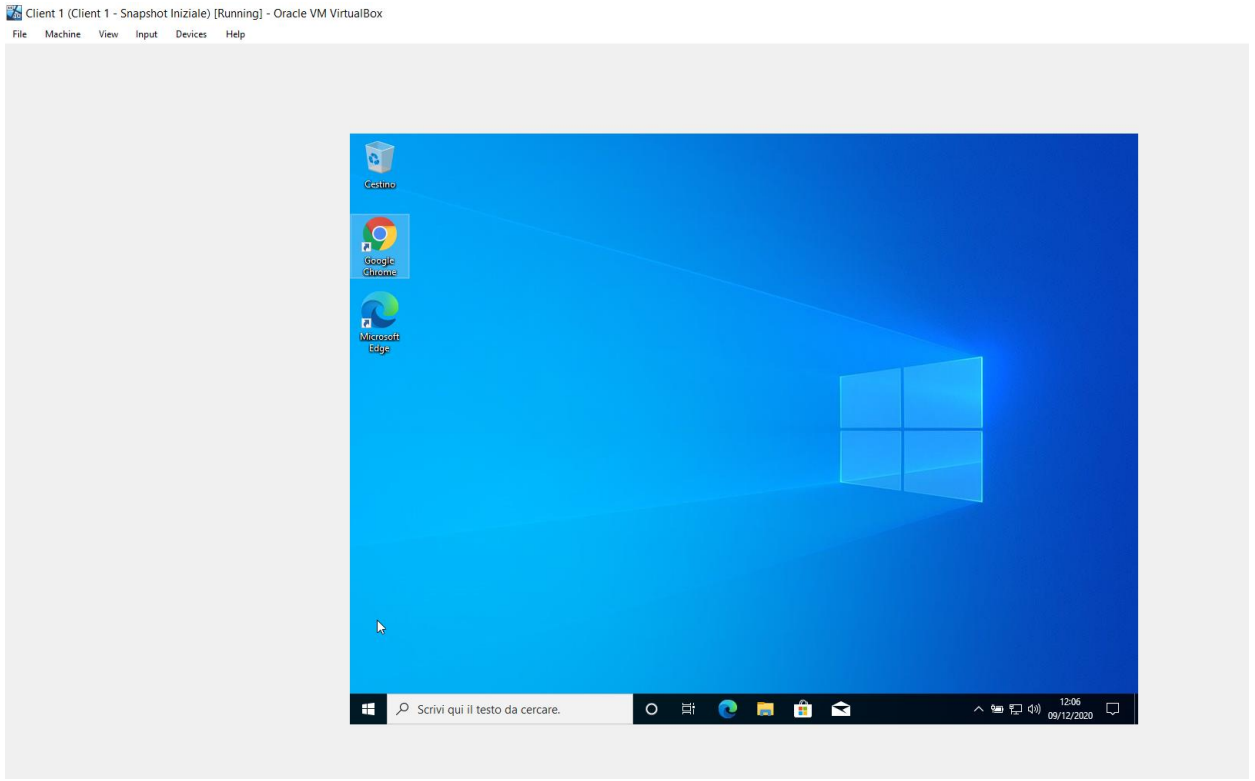
Whois Record for LatuAfiliale.com

— Domain Profile

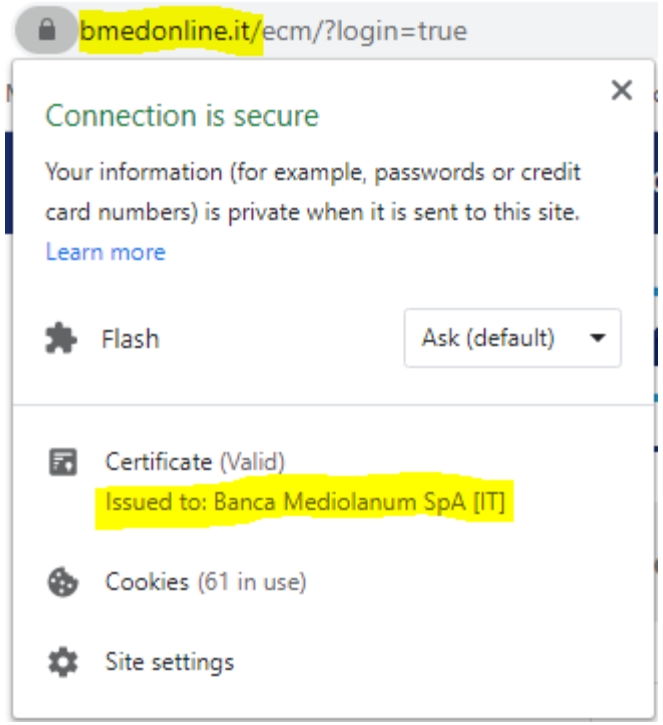
Registrant	Domain Administrator
Registrant Org	See PrivacyGuardian.org
Registrant Country	us
Registrar	NameSilo, LLC IANA ID: 1479 URL: https://www.namesilo.com/,http://www.namesilo.com Whois Server: whois.namesilo.com abuse@namesilo.com (p) 14805240066
Registrar Status	clientTransferProhibited
Dates	24 days old Created on 2020-11-15 Expires on 2021-11-15 Updated on 2020-11-16
Name Servers	NS1.QHOSTER.NET (has 6,087 domains) NS2.QHOSTER.NET (has 6,087 domains) NS3.QHOSTER.NET (has 6,087 domains) NS4.QHOSTER.NET (has 6,087 domains)
Tech Contact	Domain Administrator See PrivacyGuardian.org 1928 E. Highland Ave. Ste F104 PMB# 255, Phoenix, AZ, 85016, us pw-46badc1fd06d2a4ad044227b5864264a@privacyguardian.org (p) 13478717726

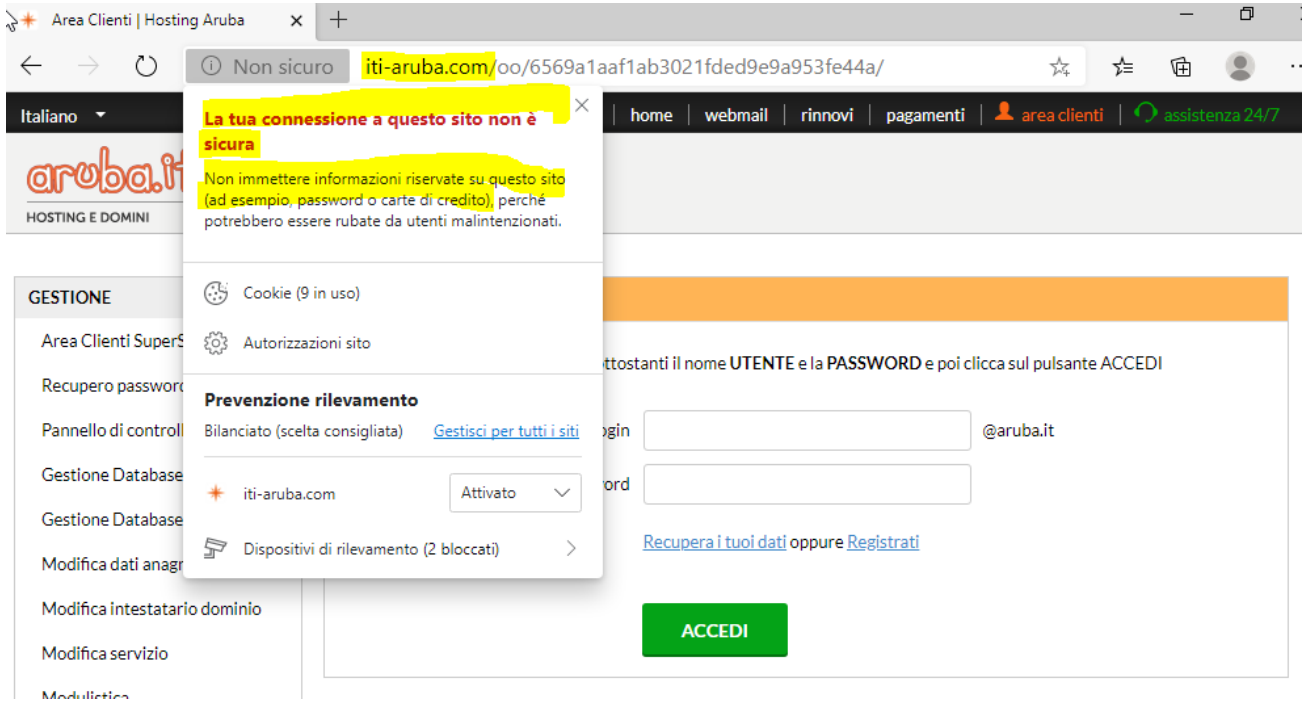
Come difendersi (sito)

- Non visitare mai l'URL indicata dal computer di lavoro
  - Utilizzare una SandBox eventualmente (macchina virtuale, computer di test, etc.)



Come difendersi - verifica certificati sito





GdL Cyber Security

Come difendersi (generale)

- Attivare MFA (Multi Factor Authentication) su email e sempre ove possibile
  - OTP (One Time Password) inviata via SMS, app di autenticazione, token
  - Microsoft Authenticator, Google Authenticator
- Effettuare scansioni AV periodiche e attivare opzioni tipo smart screen, anche con tool specifici (e.g. Malwarebytes, Spybot, hijackthis fork, etc.)
- Non fornire dati sensibili per telefono (password, PIN, etc.)
  - I codici bancari non vanno forniti mai per intero
  - Mai fornire OTP per telefono
- Non accettare contratti telefonici, chiedere sempre invio via mail
- Non consultare mail/banca su device pubblici/di altri
- Non «prestare» i propri device personali a nessuno
- Pretendere sempre una copia di ciò che si firma

Fonti

- Schema piramidale/Ponzi
- Prestazione abusiva di servizi di investimento