ARI TREVISO IQ3TR · 80° ANNIVERSARIO
CORSO A CURA DI **IK3GIG** – FABIO PROVEDEL

Sicurezza Informatica Pratica per Radioamatori

Un clic e il danno è fatto. Impara a riconoscere, prevenire e proteggere la tua stazione digitale.

PHISHING | PASSWORD SICURE | 2FA | RANSOMWARE | DARK WEB | SOFTWARE RADIO

80° ANNIVERSARIO ARI TREVISO IQ3TR

1 Perché questo ci riguarda

La cybersecurity non è più un argomento per esperti. È un elemento fondamentale della cultura personale per chiunque operi nel mondo digitale — inclusi noi radioamatori.

3°
POSTO AL MONDO PER ATTACCHI INFORMATICI SUBITI (ITALIA)

+49%
AUMENTO DEGLI INCIDENTI CYBER IN ITALIA NEL 2025 VS 2024

95%
DEGLI ATTACCHI RIUSCITI CAUSATI DA ERRORE UMANO

IL RADIOAMATORE MODERNO

Il radioamatore moderno non è più solo un operatore radio. È una figura ibrida che gestisce apparati digitali, software SDR, ripetitori via internet (Echolink, D-STAR, DMR), reti di emergenza e piattaforme online. Questa ricchezza tecnologica espone a rischi specifici.

SUPERFICIE DI ATTACCO

- Email con phishing mirato (callsign, log QSO, contest)
- Software SDR/log falsi con malware nascosto
- Database pubblici: QRZ, LoTW, eQSL
- Ripetitori Echolink/IRLP con credenziali deboli
- Reti domestiche con router mal configurati

⚠ IL CASO ARRL / LOTW

12 maggio 2024: LoTW va offline per un ransomware entrato tramite credenziali rubate sul Dark Web. ARRL ha pagato **$1.000.000** per la chiave di decifratura. Il sistema è rimasto offline per quasi **7 settimane**. Oltre 60.000 log in coda. Diplomi DXCC bloccati per mesi.

→ Se ARRL può essere colpita, chiunque di noi può esserlo.

Il messaggio chiave

La difesa parte dalle abitudini quotidiane: password uniche per ogni account, autenticazione a due fattori attiva, aggiornamenti regolari dei sistemi.

2 Come ti ingannano

> L'ingegneria sociale sfrutta la psicologia umana, non le vulnerabilità tecniche. I criminali usano leve emotive per farci abbassare la guardia — urgenza, paura, autorità, familiarità.

LEVE PSICOLOGICHE

- **Autorità:** "Sono il presidente della sezione, ho bisogno della password del ripetitore con urgenza"
- **Urgenza:** "Devi agire adesso o perdi il callsign"
- **Familiarità:** Il criminale usa il tuo nome, il tuo callsign, riferimenti al tuo ultimo contest
- **Paura:** "Il tuo computer ha un virus, chiama subito questo numero"

VARIANTI DEL PHISHING

SPEAR PHISHING

Attacco mirato verso una persona specifica, con dati personalizzati (callsign, contest, QSO recenti)

SMISHING / VISHING

Via SMS o telefonata. Es: "La sua banca ha rilevato un accesso sospetto"

QRISHING

QR code falsi applicati sopra quelli legittimi (parchimetri, locali pubblici)

📻 SCENARIO REALE PER RADIOAMATORI

Ricevi una email apparentemente da **QRZ.com**: *"Il tuo account ha rilevato accessi sospetti dalla Cina. Clicca qui per verificare la tua identità e proteggere il tuo callsign."*

- Il link porta a un sito identico a QRZ, ma falso (typosquatting)
- Inserisci le credenziali → il tuo account è compromesso
- Le credenziali vengono vendute sul Dark Web e usate per altri attacchi

SEGNALI DI ALLARME

URGENZA ARTIFICIALE

"Agisci entro 24 ore o il tuo account sarà sospeso"

MITTENTE FALSO

qrz-support@qrz**.net** invece di @qrz**.com**

ALLEGATI INATTESI

Anche da mittenti noti: potrebbero essere stati compromessi. File PDF, Excel e Word sono i più usati.

3 Come leggere un indirizzo web

Capire la struttura di un URL è la competenza più semplice e più efficace per riconoscere un sito falso. Questa è la parte più difficile — ma è quella che vi salva la vita.

ANATOMIA DI UN URL

```
https:// www. aritreviso. it /sezione/eventi

↑ protocollo   ↑ dominio 3°   ↑ dominio 2° (nome)   ↑ dominio 1°   ↑ pagina/sezione
```

⚠ Attenzione al Typosquatting — questi due link NON sono la stessa cosa!

✓ https://account.google.com/ServiceLogin

✗ https://account.google.com.ServiceLogin.it/

Nel secondo caso il dominio reale è **ServiceLogin.it**, non google.com!

COME VERIFICARE UN LINK

1. Passa il mouse sopra il link **senza cliccare**: controlla l'URL che appare in basso nel browser
2. Clic destro → "Copia collegamento" e incollalo in un file di testo per esaminarlo
3. Digita direttamente l'indirizzo nella barra del browser invece di cliccare il link nell'email
4. In caso di dubbio, incolla l'URL su **virustotal.com** per verificarlo

DOMINI TRUFFALDINI TIPICI

CARATTERI SOSTITUITI

qrz.com → qrz.corn | g0ogle.com | paypa1.com

DOMINIO AGGIUNTO

google.com.**login-verify.ru**/...

SOTTODOMINIO INGANNEVOLE

qrz.com.sicuro.**truffa.it**/login

💡 Strumento utile: VirusTotal

Prima di aprire un link sospetto o un file allegato, verificalo su **virustotal.com** — analizza con oltre 70 antivirus e blacklist. È gratuito e non richiede registrazione.

4 Il malware che cifra i tuoi file

Il ransomware è il tipo di malware più temibile: cifra tutti i tuoi file e chiede un riscatto per restituirteli. Il caso ARRL ha dimostrato che nessuno è immune — nemmeno le grandi organizzazioni.

COME ARRIVA SUL TUO PC

1. **Email con allegato:** oltre il 75% degli attacchi. File PDF, Excel, Word con macro nascoste
2. **Siti compromessi:** il "drive-by download" — basta visitare un sito infetto con browser non aggiornato
3. **Chiavette USB:** tecnica del "baiting" — trovate abbandonate in luoghi pubblici o ricevute in regalo
4. **Software cracckato:** versioni "gratuite" di programmi costosi o software radio da fonti non ufficiali

COME DIFENDERSI

- ☐ Non aprire **mai** allegati da email di dubbia provenienza
- ☐ Trattare anche email di mittenti **noti come sospette** (potrebbero essere compromessi)
- ☐ Abilitare "Mostra estensioni nomi file" in Windows — un file "documento.pdf.exe" è un eseguibile!
- ☐ **Disabilitare le macro** in Office (Word, Excel, PowerPoint)
- ☐ Fare sempre il **backup** secondo la regola 3-2-1 (3 copie, 2 supporti, 1 offsite)
- ☐ Mantenere il sistema operativo e il browser **sempre aggiornati**

📢 VETTORE SPECIFICO PER RADIOAMATORI: SOFTWARE RADIO FALSO

I criminali caricano versioni modificate dei programmi più usati su siti di terze parti e forum:

- **WSJT-X / JTDX** (FT8/FT4) – i più scaricati al mondo
- **CHIRP** – programmazione ricetrasmettitori
- **SDR#, RTL-SDR, GQRX** – driver e frontend SDR
- **N1MM, Log4OM, DXKeeper** – software contest e log

→ Regola d'oro: scarica SEMPRE dai siti ufficiali degli sviluppatori. Non installare mai software "pre-attivato" o con "patch" da forum.

💡 Regola 3-2-1 per il Backup

Mantieni
3
copie dei tuoi dati (log radio, configurazioni), su
2
supporti diversi (es. disco esterno + NAS), di cui
1
fuori sede o su cloud. Un backup non verificato è come non averlo.

5 Password sicure e autenticazione 2FA

La gestione delle password è il fondamento di ogni difesa personale. Una password riutilizzata è la porta d'ingresso principale degli attacchi ransomware — come nel caso ARRL.

QUANTO CI VUOLE A BUCARLA?

Caratteri	Solo minuscole	+ Maiusc. + Num.	+ Simboli
8	Istantaneo	2 min	5 min
10	1 min	5 giorni	2 settimane
12 ✓	14 ore	53 anni	**226 anni**
16	713 anni	779M anni	5 miliardi anni

Fonte: Hive Systems 2023. La riga evidenziata è il minimo consigliato **oggi**.

REGOLE ESSENZIALI

- ☐ Usa **password diverse** per ogni account — senza eccezioni
- ☐ Almeno **12 caratteri** con maiuscole, numeri e simboli
- ☐ Nessuna parola di dizionario, nome, data di nascita o callsign
- ☐ Usa un **password manager** (vedi sotto)
- ☐ Abilita **2FA** su tutti i servizi critici
- ☐ Verifica periodicamente su **haveibeenpwned.com**

AUTENTICAZIONE A DUE FATTORI (2FA / MFA)

1 — QUALCOSA CHE SAI

La tua password o PIN. Da sola non basta più.

2 — QUALCOSA CHE HAI

App authenticator (Google Authenticator, Microsoft Authenticator, Aegis). Preferibile agli SMS.

3 — QUALCOSA CHE SEI

Impronta digitale, riconoscimento facciale, retina.

Password Manager consigliati (gratuiti)

Bitwarden

(open source, cloud) ·

KeePassXC

(locale, offline) ·

NordPass

.

Dashlane

. Devi ricordare solo *una* master password robustissima. Il resto lo gestisce il manager, generando password casuali per ogni sito.

Attiva il 2FA anche su: QRZ.com · ClubLog · LoTW · eQSL · la tua email

Questi account contengono il tuo callsign, indirizzo, log radio e certificati DXCC. Sono un bersaglio diretto.

6 Smartphone e Dark Web

Lo smartphone è il dispositivo più vulnerabile: lo usiamo per tutto, spesso su reti Wi-Fi pubbliche, e raramente lo aggiorniamo.

JUICE JACKING

⚠ **Non usare le porte USB pubbliche!**

Le porte USB di aeroporti, treni e centri commerciali possono essere modificate per rubare dati o installare malware attraverso il cavo di ricarica. Usa **il tuo caricatore a presa elettrica** o un **power bank personale** .

DECALOGO MOBILE (SELEZIONE)

- ☐ Usa PIN robusto o biometria (mai 0000 o 1234)
- ☐ Installa app **solo** da Google Play o App Store ufficiale
- ☐ Evita Wi-Fi pubbliche; usa VPN se necessario
- ☐ Non cliccare link in SMS da numeri sconosciuti (**SMishing**)
- ☐ Verifica l'URL dei QR code prima di procedere (**QRishing**)
- ☐ Prima di cedere o vendere: ripristino di fabbrica + cancellazione SD card

COS'È IL DARK WEB

Il Dark Web è la parte nascosta di internet, non indicizzata dai motori di ricerca. Le attività sono anonime: vi si trovano mercati illegali dove vengono venduti dati rubati.

QUANTO VALGONO I TUOI DATI?

Tipo di dato	Prezzo Dark Web
Scansione passaporto UE	$3
Patente di guida fisica UE	$70
Account PayPal con saldo $1.000	~$100
5 carte di credito con dati completi	$80–$180
Credenziali domain admin azienda	**$1.000–$5.000**

🔍 **Controlla se sei stato violato**

Visita **haveibeenpwned.com** e inserisci la tua email. Se compare in una violazione nota, cambia immediatamente quella password su tutti i siti dove la usi.

7 Proteggere l'infrastruttura radio

I ripetitori connessi a internet sono infrastrutture critiche per la comunità radioamatoriale — specialmente nelle reti di emergenza. Una compromissione può bloccare comunicazioni vitali.

RISCHI PER RIPETITORI DIGITALI

ACCESSO NON AUTORIZZATO

Nodi Echolink/IRLP con password di default mai cambiate — accessibili a chiunque

DENIAL OF SERVICE

Saturazione con trasmissioni continue: blocco totale del servizio durante emergenze

CONTROLLER ESPOSTO

Interfaccia web di gestione accessibile direttamente da internet senza protezione

COME PROTEGGERE IL RIPETITORE

- ☐ **Cambia subito** tutte le credenziali di default del controller
- ☐ Non esporre l'interfaccia di gestione direttamente su internet: usa una **VPN**
- ☐ Limita i comandi DTMF critici con **codici robusti**
- ☐ Monitora regolarmente i **log di accesso** ai nodi Echolink/IRLP
- ☐ Segmenta la rete: tieni il ripetitore su una **VLAN separata**
- ☐ Aggiorna il firmware del controller quando disponibile

ROUTER DI CASA

- ☐ Cambia le credenziali di default (admin/admin)
- ☐ Aggiorna il firmware: i router vengono aggiornati raramente ma le vulnerabilità sono tante
- ☐ Disabilita servizi non necessari: Telnet, UPnP, gestione remota
- ☐ Crea una rete Wi-Fi separata (guest) per dispositivi IoT e apparati radio

INTERNET OF THINGS (IOT) — IL TALLONE D'ACHILLE DELLA RETE DOMESTICA

IL PROBLEMA

Il 57% dei dispositivi IoT è esposto a vulnerabilità note senza possibilità di aggiornamento. Telecamere, smart TV, assistenti vocali — ogni dispositivo connesso è una potenziale porta d'ingresso.

LA SOLUZIONE

Segmenta la rete: metti tutti i dispositivi IoT su una VLAN o rete Wi-Fi guest separata da PC, smartphone e apparati radio. Un device IoT compromesso non potrà raggiungere gli altri.

PER GLI APPARATI RADIO

I tuoi TRX, SDR, NAS con log radio e computer di stazione meritano una rete dedicata, isolata da internet dove possibile, con accesso limitato.

8 Sono stato attaccato: i primi passi

La velocità di reazione è fondamentale. I primi minuti dopo la scoperta di un attacco determinano l'entità del danno. Ecco le azioni da compiere nell'ordine corretto.

1. **Disconnetti il dispositivo dalla rete** (cavo di rete + Wi-Fi). Non spegnerlo: potresti perdere prove forensi utili per le indagini.
2. **Cambia le password da un dispositivo diverso e sicuro** (smartphone su dati mobili). Inizia dall'email principale, poi account bancari, poi tutto il resto.
3. **Avvisa gli altri** che potrebbero essere stati coinvolti: soci del club, utenti del ripetitore. Il tuo account compromesso potrebbe inviare phishing a tuo nome.
4. **Segnala l'incidente alla Polizia Postale** su **www.commissariatops.it**. Denuncia obbligatoria in caso di frode finanziaria; consigliata in tutti gli altri casi.
5. **Contatta la tua banca** se dati finanziari o account di pagamento potrebbero essere stati compromessi. Blocca carte preventivamente.
6. **Documenta tutto:** screenshot degli eventi anomali, email ricevute, orari, log di sistema. La documentazione è essenziale per le indagini e per la denuncia.

In caso di ransomware: NON pagare subito

Contatta prima un professionista e verifica su **nomoreransom.org** se esiste una chiave di decifratura gratuita. Pagare non garantisce il recupero dei dati e finanzia i criminali.

Il Ciclo dell'Attacco

Gli attacchi mirati seguono un processo:
Ricognizione (QRZ, social, forum) → **Pretesto** → **Attacco** → **Sfruttamento** → **Persistenza** → **Cancellazione tracce**. Conoscerlo aiuta a riconoscerlo.

IL PROBLEMA È TRA LA TASTIERA E LA SEDIA

PEBKAC — "PROBLEM EXISTS BETWEEN KEYBOARD AND CHAIR"

Il 95% degli attacchi informatici andati a buon fine ha come causa almeno un errore umano. Non è una questione di tecnologia — è una questione di consapevolezza e abitudini. La formazione che hai ricevuto oggi è la tua principale difesa. **Condividila con la tua famiglia e i tuoi colleghi di sezione.**

9 Decalogo del radioamatore digitale sicuro

- ☐ Usa **password diverse** per ogni account (QRZ, LoTW, eQSL, email, router)
- ☐ Attiva **2FA** su tutti i servizi critici: email, LoTW, QRZ, PayPal
- ☐ Usa un **password manager** (Bitwarden, KeePassXC)
- ☐ Scarica software radio **SOLO dai siti ufficiali**. Verifica il checksum MD5/SHA256
- ☐ Aggiorna il firmware del router e cambia le **credenziali di default**
- ☐ Cambia le credenziali di default del controller del ripetitore. **Non esporlo su internet**
- ☐ Verifica se le tue email sono state compromesse su **haveibeenpwned.com**
- ☐ Prima di cliccare un link, **verifica sempre l'URL reale**. Diffida delle urgenze via email
- ☐ Non condividere mai credenziali via WhatsApp, Telegram o email, **neanche con amici**
- ☐ In caso di attacco: disconnetti, cambia password da altro dispositivo, segnala a **Polizia Postale**

RISORSE UTILI

RISORSA	URL	DESCRIZIONE
Have I Been Pwned	haveibeenpwned.com	Verifica se la tua email è stata violata in un data breach
VirusTotal	virustotal.com	Analizza file e URL sospetti con oltre 70 antivirus
No More Ransom	nomoreransom.org	Chiavi di decifratura gratuite per ransomware noti
Commissariato PS Online	commissariatops.it	Polizia Postale — denuncia crimini informatici online
CLUSIT	clusit.it	Rapporto annuale sulla cybersicurezza in Italia
Bitwarden	bitwarden.com	Password manager open source gratuito
KeePassXC	keepassxc.org	Password manager locale, offline, open source
ACN Italia	acn.gov.it	Agenzia per la Cybersicurezza Nazionale

📻 PER I LOG RADIO

Backup regolare di log, ADIF export, configurazioni WSJT-X/JTDX e certificati LoTW su supporto esterno offline.

🔄 AGGIORNAMENTI

Sistema operativo, browser, antivirus, router firmware: imposta aggiornamenti automatici dove possibile.

🤝 CONDIVIDI

Parla di sicurezza informatica agli altri soci della sezione. La consapevolezza collettiva è la miglior difesa.