

POMONA RATGEBER

Dienstag, 31. März 2026
ab 18.30 Uhr im
1815.träff in
Brig-Glis



UNSER EXPERTE

Michael Buri ist Bereichsleiter Schulungen und Privatkundenberater im grössten Oberwalliser Informatikunternehmen und weist eine breite Erfahrung über das Themengebiet auf. Er kann Ihnen viele Ratschläge und Tipps rund um das Thema IT-Sicherheit vermitteln. Seien Sie live am Pomona Ratgebertreffen vom **31. März im 1815.träff** in Brig-Glis dabei. (Anmeldung unter pomona-ratgeber.ch)

LIEBE POMONA-MEDIA-NUTZERINNEN

Auf Pomona-Ratgeber.ch werden regelmässig wissenswerte und alltägliche Themen behandelt, zu denen Experten zu treffenden Fragen Stellung nehmen. Der Experte wird dann eine Woche nach Beginn der Ankündigung (im «Walliser Boten», auf www.walliserbote.ch und www.rro.ch) das Thema rund um die Antworten vertiefen.

Weitere Informationen finden Sie unter www.pomona-ratgeber.ch (direkt über diesen QR-Code), wo Sie sich auch direkt anmelden können (Anmeldefrist Montag, 30. März)



Wir freuen uns auf Sie!

Cybersicherheit – Wie schütze ich mich vor virtuellen Gefahren?

In einer Welt, in der die Digitalisierung allgegenwärtig ist, wird das Thema Cybersicherheit zu einer zunehmenden Herausforderung für uns alle. Ein verantwortungsvoller Umgang mit Technologie ist deshalb wichtiger denn je. Jeder kann zur eigenen digitalen Sicherheit beitragen, indem grundlegende Schutzmassnahmen beachtet und potenzielle Risiken aufmerksam wahrgenommen werden. Unser Experte Michael Buri weiss sehr genau, worauf man dabei achten sollte.

Pomona-Ratgeber:

Was für Arten von virtuellen Gefahren gibt es eigentlich?

Michael Buri: Virtuelle Gefahren umfassen eine Vielzahl digitaler Bedrohungen, die darauf abzielen, Daten zu stehlen, Systeme zu beschädigen oder Nutzer zu täuschen. Im Groben kann man diese in die fünf Hauptkategorien einteilen:

- Schadsoftware
- Phishing und Social Engineering
- Netzwerkangriffe
- Daten- und Identitätsmissbrauch
- Cybermobbing, Belästigungen und Love Scam

Was versteht man allgemein unter Cybersicherheit?

Michael Buri: Cybersicherheit umfasst allgemein alle Technologien, Prozesse und Praktiken, die darauf abzielen, Computernetzwerke, Geräte, Programme und Daten vor Cyberbedrohungen zu schützen.

Warum nimmt die Bedeutung von Cybersicherheit stetig zu?

Michael Buri: Durch die zunehmende und schnellere Vernetzung steigt auch die Angriffsfläche im Verhältnis exponentiell an. Cyberkriminalität wird dadurch immer komplexer und vielschichtiger. Jeder vernetzte Aspekt, von Online-Konten bis zu smarten Geräten, kann ein Einfallstor für Phishing, Malware oder Datenlecks sein. Ausserdem finden Cyberkriminelle immer neue Wege und Möglichkeiten, uns zu täuschen.

Welche grundlegenden Massnahmen kann jeder im Alltag umsetzen, um sich zu schützen?

Michael Buri: In erster Linie hilft es schon, wenn jeder sein Onlineverhalten hinterfragt. Misstrauen, Vorsicht und gesunder Menschenverstand gehören genauso dazu wie die regelmässige Aktualisierung der verwendeten Software und das regelmässige Durchführen von Backups.

Welche Rolle spielen Passwörter für die persönliche digitale Sicherheit?

Michael Buri: Passwörter sind ein Eckpfeiler der persönlichen digitalen Sicherheit und dienen als erste Verteidigungslinie gegen unbefugten Zugriff auf Ihre Online-Konten. Eigentlich weiss mittlerweile jeder, wie ein sicheres Passwort aussehen sollte, dennoch wird es oft aus Bequemlichkeit oder Angst vor Vergessen möglichst simpel gehalten.

Wie kann man Phishing-Angriffe erkennen und vermeiden?

Michael Buri: Das Wichtigste ist sicherlich, sensibilisiert zu sein und auf typische Warnsignale zu achten. Dazu gehören zum Beispiel: dringender Handlungsbedarf (Drohungen, kurze Fristen), ungewöhnliche Absenderadressen, eine allgemeine oder fehlerhafte Anrede, schlechte Rechtschreibung, die Aufforderung zur Eingabe von Passwörtern oder zum Öffnen von Links bzw. Anhängen. Die beste Verteidigung ist Wachsamkeit in Kombination mit technischen Schutzmassnahmen.

Warum sind regelmässige Software-Updates so wichtig?

Michael Buri: Regelmässige Software-Updates sind entscheidend, weil sie Sicherheitslücken schliessen, die Angreifer für Malware und Hacks nutzen könnten.

Zudem beheben Updates Fehler, verbessern die Stabilität und Leistung und bringen oft neue Funktionen oder Verbesserungen, die die Benutzerfreundlichkeit und Produktivität erhöhen.

Welche Bedeutung haben Antivirenprogramme und Firewalls?

Michael Buri: Antivirenprogramme und Firewalls sind grundlegende Pfeiler der Cybersicherheit. Firewalls fungieren als Netzwerk-Wächter, blockieren unerwünschten Datenverkehr und verhindern unbefugten Zugriff.

Die Antivirensoftware erkennt Malware wie Viren, Trojaner oder Ransomware, und isoliert sie, bevor sie Schaden anrichten kann.

Inwiefern beeinflusst menschliches Verhalten die Cybersicherheit?

Michael Buri: Der Mensch ist ein zentraler Faktor der Cybersicherheit – oft sogar der kritischste. Fehlendes Wissen, hohe Arbeitsbelastung oder mangelnde Sensibilität für Sicherheitsthemen bergen erhebliche Risiken.

Welche Risiken entstehen durch ungesicherte WLAN-Netzwerke?

Michael Buri: Ungesicherte WLAN-Netzwerke, insbesondere öffentliche, bergen erhebliche Sicherheitsrisiken, da der Datenverkehr meist unverschlüsselt übertragen wird. Cyberkriminelle können dies ausnutzen, um sensible Informationen abzufangen oder Malware zu verbreiten.

Welche Daten sind besonders schützenswert und warum?

Michael Buri: Besonders schützenswert sind sensible Informationen wie Gesundheits-, genetische oder biometrische Daten, ethnische Herkunft, politische oder religiöse Ansichten sowie Angaben zum Sexualleben.

Ihr Missbrauch kann zu Diskriminierung, Ausgrenzung oder schwerwiegenden Persönlichkeitsverletzungen führen und tief in die Grundrechte eingreifen.

GESTALTE MIT UNS SICHERE IT-LÖSUNGEN.

Bewirb dich auf ocom.ch/karriere