

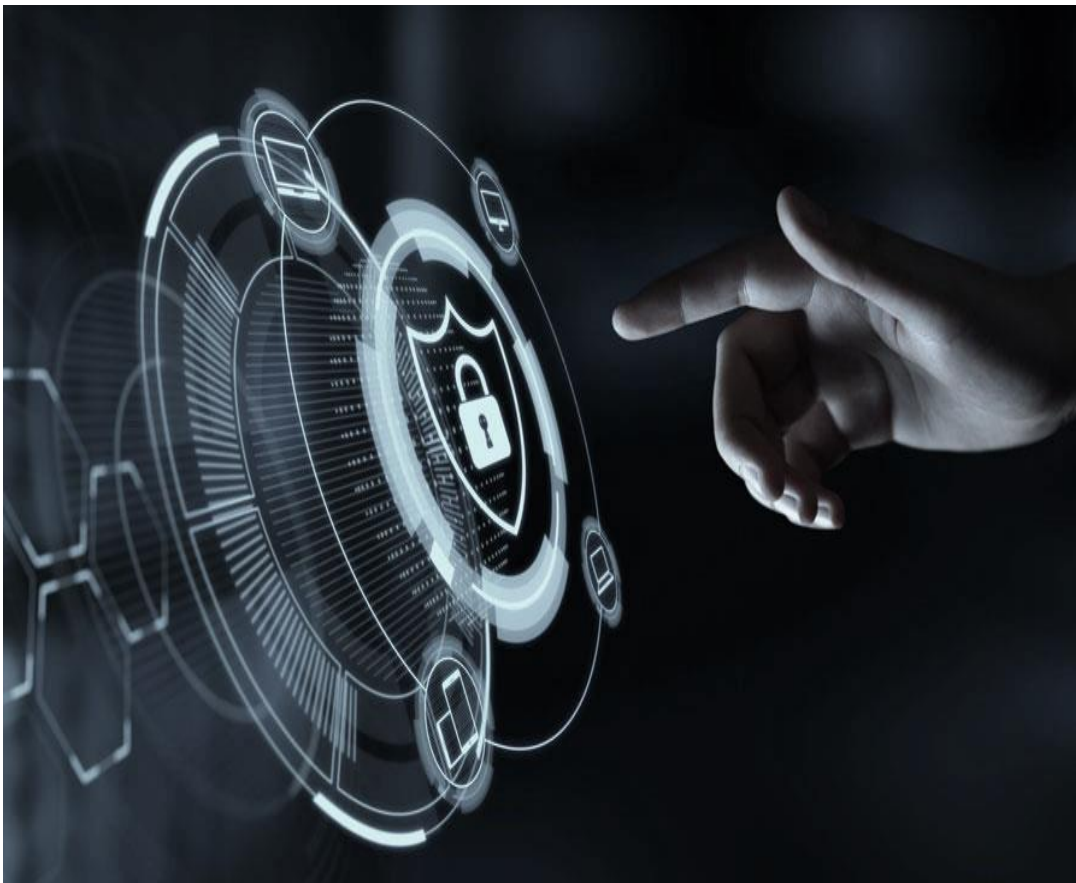
PG LEGAL INSURANCE NEWS ALERT



pg legal

- **CYBERNETIC SECURITY DURING THE COVID-19 DAYS**
- **LA SICUREZZA CIBERNETICA AI TEMPI DEL COVID-19**

May 2020



*“more than 20 years of advising
insurance & reinsurance
business”*

GIOVANNA AUCONE
Partner
Email:aucone@pglegal.it

GIANFRANCO PUOPOLO
Partner
Email:g.puopolo@pglegal.it

Milan
Via Sant'Andrea,3
20121 Milan, Italy
T: +39 02 760 13359
F: +39 02 760 27478

Rome
Via Ombrone,14
00198 Rome, Italy
T: +39 06 884 1535
F: +39 06 884 2094

Dublin
77 Sir John Rogersons Quay,
Block C, Grand Canal Docklands,
Dublin 2, D02 VK60, Ireland
T: +353 (0) 1 571 8019

Also in Naples and Genoa



pglegal.it



CYBERNETIC SECURITY DURING THE COVID-19 DAYS

On 20 April 2020, the Cyber Security Coordination Group - created by IVASS and the Bank of Italy - intervened on the subject of cyber security at the time of Covid-19.

The emergency situation has contributed to accelerating the process of digitization of economies, introducing, however, new cybernetic risks. A greater digitization, in fact, if on the one hand means more productivity, less pollution and easier balance between life and work, on the other hand it leads to an increased **risk of cyber-attacks**.

This is what emerges from the article "Cyber security in the days of Covid -19" in which it is also stated that those who are particularly exposed are the people and companies who in the past made modest use of the network and who are not always aware of the dangers of the digital world.

Therefore, the Bank of Italy and IVASS have, as a consequence, strengthened the protection of the internal information systems and, within the scope of institutional competences, the security of the financial and insurance system, with particular attention to the protection of individuals and companies who, before the epidemic, made modest recourse to the network.

In particular, following the diffusion, by cyber criminals, of numerous fraudulent e-mail messages which publicize self-styled cures against the Coronavirus or fictitious solidarity initiatives, in an attempt to steal from the recipients sums of money and credentials of access to the online accounts (so-called phishing), **the two Institutions have increased the safeguards for the protection of cybernetic security**.

In this regard, in fact, the CERTBI of the Information Technology Department - Computer Emergency Response Team (CERTBI), part of the internal controls of the Bank (CERTBI) - is conducting, in addition to its ordinary activity, targeted analyses on the characteristics of these threats (cyber threat intelligence), also on the basis of the continuous sharing of information with trusted counterparts and technological partners (infosharing). With regard to the risks deriving from telework, it is engaged in interventions to raise risk awareness (security awareness) in favour of the Bank's and IVASS's staff.

CERTFin - Computer Emergency Response Team of the Italian financial sector - in collaboration with other institutions, is helping to strengthen the defenses of the national financial system, through tools such as infosharing between



intermediaries, the dissemination of security bulletins, the organization of webinars on attack techniques, the possible countermeasures to be taken, training on the proper use of corporate devices and the strengthening of controls related to remote work.

LA SICUREZZA CIBERNETICA AI TEMPI DEL COVID-19

In data 20 aprile 2020, il Gruppo di coordinamento per la sicurezza cibernetica – costituito da IVASS e Banca d'Italia – è intervenuto in merito alla tematica della sicurezza cibernetica ai tempi del Covid- 19.

La situazione emergenziale ha concorso ad accelerare la digitalizzazione delle economie, introducendo, tuttavia, nuovi rischi cibernetici. Una maggiore digitalizzazione, infatti, se da un lato equivale a più produttività, meno inquinamento e più agevole conciliazione tra vita e lavoro, dall'altro comporta un aumento **del rischio di attacchi informatici**.

E' quanto emerge dall'articolo "La sicurezza cibernetica ai tempi del Covid -19" nel quale si legge altresì che ad essere particolarmente esposte sono le persone e le imprese che in passato facevano ricorso alla rete in misura modesta e che non sempre hanno consapevolezza dei pericoli del mondo digitale.

Pertanto, Banca d'Italia e IVASS hanno, di conseguenza, rafforzato la protezione dei sistemi informatici interni e, nell'ambito delle competenze istituzionali, la sicurezza del sistema finanziario e assicurativo, con precipua attenzione proprio alla tutela di soggetti ed imprese che, prima dell'epidemia, facevano un modesto ricorso alla rete.

In particolare, in seguito alla diffusione, da parte di criminali informatici, di numerosi messaggi di posta elettronica fraudolenti che pubblicizzano sedicenti cure contro il Coronavirus o fittizie iniziative di solidarietà, nel tentativo di sottrarre ai destinatari somme di denaro e credenziali di accesso ai conti online (c.d. phishing), **le due Istituzioni hanno incrementato i presidi a tutela della sicurezza cibernetica**.

Al riguardo, infatti, il CERTBI del Dipartimento Informatica - Computer Emergency Response Team (CERT), parte dei presidi interni della Banca (CERTBI) – sta conducendo, in aggiunta all'attività ordinaria, approfondimenti mirati sulle caratteristiche di queste minacce (*cyber threat intelligence*), anche sulla base della continua condivisione di informazioni con controparti fidate e *partner* tecnologici (*infossharing*). Quanto ai rischi derivanti dal telelavoro, è impegnato in interventi di innalzamento della consapevolezza del rischio (*security awareness*) in favore del



personale della Banca e dell'IVASS.

Il CERTFin - Computer Emergency Response Team del settore finanziario italiano- in collaborazione con altre istituzioni, sta contribuendo a rafforzare le difese del sistema finanziario nazionale, mediante strumenti quali l'*infosharing* tra intermediari, la diffusione di bollettini di sicurezza, l'organizzazione di *webinar* sulle tecniche di attacco, le possibili contromisure da adottare, la formazione sul corretto utilizzo dei dispositivi aziendali e il rafforzamento dei presidi connessi al lavoro da remoto.

For more information and further clarifications please contact:

GIOVANNA AUCONE

Partner

E: aucone@pglegal.it

GIANFRANCO PUOPOLO

Partner

E: g.puopolo@pglegal.it

pglegal.it

© 2020 PG Legal is PG Legal Studio Legale Associato. All rights reserved

Whilst every care has been taken to ensure the accuracy of this information at the time of publication, the information is intended as guidance only. It should not be considered as legal advice.

PG Legal is the Data Controller for any data that it holds about you in accordance with GDPR. We use cookies and tracking technology to see whether emails are opened or replied to, and whether links are followed. This information helps us to improve the services we offer and to tailor our communications with you. To unsubscribe, change your mailing preferences, correct your personal details, request a copy of your personal details, or ask us to delete or stop processing your personal details please use the link [unsubscribe](#) or contact info@pglegal.it