PRESS RELEASE

CYBER CRIME: DECEMBER WORST MONTH OF 2020

Exprivia's Cybersecurity Observatory registers a rise in cyber crimes in the final quarter of the year almost five times that of the first quarter.
Finance is one of the worst hit sectors, mainly due to the increase in cashless payments.
Email and social networks the main traps. Medical devices targeted.

24 February 2021 – After months of fluctuation, back on the rise at the end of the year are **cyber crimes in Italy**; with a peak in December, 2020 was a complex year also with regard to online security.

According to the final report of 2020 on cyber threats **in Italy** drawn up by **Exprivia's Cybersecurity Observatory**, in the **October-December** period 237 cyber crimes were recorded, up by 60% on the previous quarter and almost 400% on the January-March period, when there were only 49. March marked the watershed in the rise in cyber crime: with the start of the **pandemic** and the resulting spread of **smart working**, there was an upsurge in cyber attacks, privacy breaches and incidents in all sectors of the economy and the public administration.

Exprivia's Observatory - engaged in spreading the culture of cyber security – reports that the phenomena, besides the **huge number of devices connected to the internet**, are linked to the exponential growth in **digital transactions**, including online shopping and bank transactions, especially in the last part of the year. In particular, according to the report - which examined over 50 public sources of information - the month of **December** is, with 96 crimes, the one that registered the **record number of the year**.

“While the pandemic accelerated the digitisation of our country, internet security was seriously put to the test - **stated Domenico Raguseo, Exprivia's Cybersecurity Director.** *What surprised us the most was that the weakness most exploited by attackers is the human factor. So all of us – Raguseo adds - must be aware of the risks that exist online and begin to be wary of anomalies. For example, of the unexpected videos or gifs we receive on instant messaging apps, of the syntax errors contained in suspect emails, of fake domains in email addresses or of the sudden speed with which we can browse on the pc. We are the first to be able to protect ourselves from attackers”.*

Throughout 2020, over 60% of crimes resulted in **data theft**, greatly exceeding both **privacy breaches** (13% of cases) – almost **tripled since the start of the year** – and **money losses** (10%).

The techniques most exploited by cybercriminals during 2020 count firstly **phishing-social engineering with 43% of cases**, which particularly affects distracted users or those with little knowledge of how to spot traps via email or social networks. Following this technique are **unknowns**(24% of total events), namely new methodologies tested by hackers to avoid being detected by traditional defence mechanisms, and **malware** (23%), whose use has quadrupled over the course of the year.

In 2020 the **Public Administration** and the **Finance** sector were the most vulnerable **areas and most attacked by cybercriminals,** with recorded events being 91 and 81 respectively. Thought-provoking figures, considering the acceleration in the **digitalisation of PA services, in the use of banking applications and of digital payments.** And highlighted in the financial sphere, particularly vulnerable due to the exposure of sensitive data often without proper protection, is an exponential increase in such phenomena during the year, from the single episode registered between January and March, to 41 in the final quarter, half of all crimes detected in the sector in 2020.

Next, **with 41 episodes**, is **Education**, targeted due to the mass use of remote learning by schools and universities. No less hit is the **Industry** sector which having registered incremental peaks throughout the year, counted **17 crimes in the final quarter alone, almost 50% of the whole of 2020**, caused by an increase in devices connected to the net, many without authentication, and also by many episodes of industrial espionage.

In the spotlight of Exprivia's Cybersecurity Observatory are the cybercrime episodes in **Healthcare** which, hard hit in the middle months of the year, is not on the podium for the number of crimes suffered but deserves attention for the **seriousness** of those crimes, if we consider the value of **healthcare data stolen and used on the 'dark web'.** Also emerging from analysis by Exprivia experts, last year **medical devices** were exposed to many weaknesses, starting with personal devices used by doctors and patients for remote assistance. In fact, cyber criminals can take **control of a device by blocking the service** or by tampering with its functions, for the purpose of acquiring sensitive information.

Lastly, experts at Exprivia underline that in the whole year **cyber attacks** increased by almost eight times compared to the first January-March quarter **(from 25 to 199)**, while **incidents**, namely attacks that are successful, fluctuated with a peak between April and June (46) and a drop in the months to follow, going down by **40%** between the second and the fourth quarter of the year. The attacking techniques are probably more and more complex and it is more difficult to identify cyber criminals effectively and put an actual number on the incidents.

In addition to the report, the Exprivia website www.exprivia.it also has a list of courses organised for training in the field of IT security and risk management.

PRESS RELEASE

Exprivia

Exprivia is the parent company of an international group specialized in Information and Communication Technology able to direct drivers of change in the business of its customers thanks to digital technologies.

With a consolidated know-how and a long experience due to the constant presence on the market, the group has a team of experts specializing in various fields of technology and in the main areas within this sector, from the Capital Market, Credit & Risk Management to IT Governance, from BPO to IT Security, from Big Data to Cloud, from IoT to Mobile, from networking to enterprise collaboration to SAP. The group supports its clients in the Banking & Finance, Telco & Media, Energy & Utilities, Aerospace & Defense, Manufacturing & Distribution, Healthcare and Public-Sector sectors. The group offering is made up of solutions that are composed of third-party products, engineering services and consultancy.

Following the acquisition of 81% of Italtel's share capital, an historic Italian company that today operates in the ICT market with a strong focus on the Telco & Media, Enterprises and Public-Sector markets, today the group has about 3,600 professionals distributed in over 20 countries worldwide.

Exprivia S.p.A. is listed on Borsa Italiana Stock Exchange to the MTA market (XPR).

Exprivia is subject to the direction and coordination of Abaco Innovazione S.p.A.

www.exprivia.it/en

Contacts

Exprivia SpA	Press office
Investor Relations Gianni Sebastiano gianni.sebastiano@exprivia.com T. + 39 0803382070 - F. +39 0803382077	**Sec Mediterranea** T. +39 0805289670 Teresa Marmo marmo@secrp.com Cell. +39 3356718211 Gianluigi Conese conese@secrp.com Cell. +39 3357846403 **Sec and Partners** T. +39 063222712 Martina Trecca trecca@secrp.com Cell. +39 3339611304 Andrea Lijoi lijoi@secrp.com Cell. +39 3292605000