IBM Newsroom

IBM Survey: Pandemic-Induced Digital Reliance Creates Lingering Security Side Effects

- Individuals created 15 new accounts on average during the pandemic according to survey, with 82% reusing passwords across accounts

- More than half of millennials surveyed would rather place an order using a potentially insecure app or website vs. call or visit a location in person

CAMBRIDGE, Mass., June 15, 2021 /PRNewswire/ -- IBM (NYSE: IBM) Security today announced the results of a global survey examining consumers' digital behaviors during the pandemic, as well as their potential long-term impact on cybersecurity. With society becoming increasingly accustomed to digital-first interactions, the study found that preferences for convenience often outweighed security and privacy concerns among individuals surveyed – leading to poor choices around passwords and other cybersecurity behaviors.

Consumers' lax approach to security, combined with rapid digital transformation by businesses during the pandemic, may provide attackers with further ammunition to propagate cyberattacks across industries – from ransomware to data theft. According to IBM Security X-Force, bad personal security habits may also carry over to the workplace and can lead to costly security incidents for companies, with compromised user credentials representing one of the top root sources of cyberattacks reported in 2020.[1]

The global survey[2] of 22,000 individuals in 22 markets, conducted by Morning Consult on behalf of IBM Security, identified the following effects of the pandemic on consumer security behaviors:

- **Digital Boom will Outlast Pandemic Protocols:** Individuals surveyed created 15 new online accounts during the pandemic on average, equating to billions of new accounts created around the world. With 44% reporting that they do not plan to delete or deactivate these new accounts, these consumers will have an increased digital footprint for years to come, greatly expanding the attack surface for cybercriminals.
- **Account Overload Led to Password Fatigue:** The surge in digital accounts led to lax password behaviors among those surveyed, with 82% of respondents admitting to reusing credentials at least some of the time. This means that many of the new accounts created during the pandemic likely relied on reused email and password combinations, which may have already been exposed via data breaches over the past decade.
- **Convenience Often Outweighed Security & Privacy:** More than half (51%) of millennials surveyed would rather place an order using a potentially insecure app or website, rather than call or go to a physical location in person. With these users more likely to overlook security concerns for the convenience of digital ordering, the burden of security will likely fall more heavily on companies providing these services to avoid fraud.

As consumers lean further into digital interactions, these behaviors also have the potential to spur adoption of emerging technologies in a variety of settings – from telehealth, to digital identity.[3]

"The pandemic led to a surge in new online accounts, but society's growing preference for digital convenience may come at a cost to security and data privacy," said Charles Henderson, Global Managing Partner and Head of IBM Security X-Force. "Organizations must now consider the effects of this digital dependence on their security risk profile. With passwords becoming

less and less reliable, one way that organizations can adapt, beyond multi-factor authentication, is shifting to a zero trust approach – applying advanced AI and analytics throughout the process to spot potential threats, rather than assuming a user is trusted after authentication."

Consumers Report High Expectations for Ease of Access

The survey shed light on a variety of consumer behaviors impacting the cybersecurity landscape today and moving forward. As individuals increasingly embrace digital interactions in more realms of their lives, the survey found that many have also become primed with high expectations for ease of access and use.

- **5 Minute Rule:** According to the survey, most adults (59%) expect to spend less than 5 minutes setting up a new digital account.
- **Three Strikes, You're Out:** Globally, respondents would attempt 3-4 logins before resetting their password. These resets not only cost companies' money, but they can also pose security threats if used in combination with an already compromised email account.
- **Committed to Memory:** 44% of respondents store online account information in their memory (most common method,) while 32% write this information on paper.
- **Multi-factor Authentication:** While password reuse is a growing problem, adding an additional factor of verification for higher risk transactions can help reduce the risk of account compromise. The survey found that around two-thirds of global respondents had used multi-factor authentication within the past few weeks of being surveyed.

Diving Deeper into Digital Healthcare

During the pandemic, digital channels became a crucial component to address massive demands for COVID-19 vaccines, testing and treatment. Consumers' adoption of a wide variety of digital channels for COVID-19-related services may spur greater digital engagement with healthcare providers moving forward by lowering the barrier for entry among new users, according to IBM Security analysis.[4] According to the survey:

- 63% of respondents engaged with pandemic-related services[5] via some form of digital channel (web, mobile app, email, and text message).
- While websites/web apps were the most common method of digital engagement, mobile apps and text messages also received significant usage – with 39% and 20% engaging via these channels, respectively.

As healthcare providers push further into telemedicine, it will become increasingly important for their security protocols to be designed to withstand this shift – from keeping critical IT systems online, to protecting sensitive patient data and continued HIPAA compliance. This includes data segmentation and implementing strict controls so that users can only access specific systems and data, limiting the impact of a compromised account or device. To prepare for the event of ransomware and extortion attacks, patient data should be encrypted, preferably at all times, and there must be reliable backups in place so that systems and data can be quickly restored with minimal interruption.

Paving the Way for Digital Credentials

The concept of digital health passes, or so-called vaccine passports, introduced consumers to a real-world use case for digital credentials, which offer a technology-based approach to verify specific aspects of our identity. According to the survey, 65% of adults globally say they are familiar with the concept of digital credentials, and 76% would be likely to adopt them if they became commonly acceptable.

This exposure to the idea of digitized proof of identity during the pandemic may help spur wider adoption of modernized

systems of digital identity, which could potentially replace the need for traditional forms of ID like passports and driver's licenses, offering a way for consumers to provide the limited information required for a specific transaction. While leveraging a digital form of identity has the potential to create a sustainable model for the future, security and privacy measures must be put in place to help protect against counterfeiting – calling for the capabilities of blockchain solutions to verify and provide the ability to update these credentials in the event they are compromised.

How Organizations Can Adapt to Shifting Consumer Security Landscape

Businesses that have become increasingly reliant on digital engagement with consumers as a result of the pandemic should consider the impact this has on their cybersecurity risk profiles. In light of shifting consumer behaviors and preferences around digital convenience, IBM Security suggests that organizations consider the following security recommendations:

- **Zero Trust Approach:** Given increasing risks, companies should consider evolving to a zero trust security approach, which operates under the assumption that an authenticated identity or the network itself may already be compromised, and therefore continuously validates the conditions for connection between users, data and resources to determine authorization and need. This approach requires companies to unify their security data and approach, with the goal of wrapping security context around every user, every device and every interaction.
- **Modernizing Consumer IAM:** For companies that want to continue leveraging digital channels for consumer engagement, providing a seamless authentication process is important. Investing in a modernized Consumer Identity and Access Management (CIAM) strategy can help companies increase digital engagement – providing a frictionless user experience across digital platforms and using behavioral analytics to help decrease the risk of fraudulent account use.
- **Data Protection & Privacy:** Having more digital users means that companies will also have more sensitive consumer data to protect. With data breaches costing companies $3.86 million on average among those studied,[6] organizations must put strong data security controls in place to protect against unauthorized access – from monitoring data to detect suspicious activity, to encrypting sensitive data wherever it travels. Companies should also implement the right privacy policies on-premises and in the cloud in order to help maintain consumer trust.
- **Put Security to the Test:** With usage and reliance on digital platforms changing rapidly, companies should consider dedicated testing to verify that the security strategies and technologies they've relied on previously still hold up in this new landscape. Re-evaluating the effectiveness of incident response plans and testing applications for security vulnerabilities are both important components of this process.

To view the full report, please visit:http://ibm.biz/IBMSecurity_ConsumerSurvey

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM Security X-Force® research, enables organizations to effectively manage risk and defend against emerging threats. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 150 billion+ security events per day in more than 130 countries, and has been granted more than 10,000 security patents worldwide. For more information, please check www.ibm.com/security, follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog.

***Report Methodology**: A global survey was conducted by Morning Consult on behalf of IBM in March 2021. The study was conducted among 22,000 adults in 22 markets (1,000 respondents per market) including Argentina, Australia, Brazil, Canada, Chile, Colombia, France, Germany, India, Italy, Japan, Mexico, Peru, Singapore, South Korea, Spain, UK, US, Middle East, Central & Eastern Europe, Nordics, and BNL (Belgium, Netherlands, and Luxembourg).*

###

Media Contact:
Cassy Lalan
IBM Security Communications
319-230-2232
cllalan@us.ibm.com

---

[1] IBM X-Force Threat Index 2021: Compromised user credentials were #3 initial attack vector for cyberattacks in 2020, representing 18% of incidents reported.

[2] Global survey was conducted by Morning Consult on behalf of IBM in March 2021. The study was conducted among 22,000 adults in 22 markets.

[3] Prediction based on IBM Security insights

[4] Prediction based on IBM Security analysis

[5] Includes COVID-19 financial relief, testing, treatment and vaccinations

[6] 2020 Cost of a Data Breach Report, benchmark study conducted by Ponemon Institute, analyzed and sponsored by IBM Security

SOURCE IBM

Additional assets available online: Photos

https://stage.mediaroom.com/ibmnewsroom/2021-06-15-IBM-Survey-Pandemic-Induced-Digital-Reliance-Creates-Lingering-Security-Side-Effects