BANK OF AMERICA

CYBER SECURITY

Be Cyber Secure: Cloud Computing

Tips to protect yourself, and how to respond if you think you have been targeted.

Cloud computing services make it easy to store, retrieve and share files, no matter where you are. They are also a good way to back up important information. Although most cloud providers have tools to help keep data safe, they can still be targeted by cyber criminals, so it is important that you help protect your and your company's data.

How to Protect Yourself

Be proactive:

- **Use secure, complex and unique passwords** for your cloud login, and change them frequently. Use multifactor authentication when possible.
- **Adjust user permissions,** which are a major cause of data breaches. Not everyone authorized to log in to your cloud account needs to have access to every file, service or function.
- **Secure data by encrypting** both while sending it to the cloud and when storing it there to prevent cyber criminals accessing your information in transit.
- **Understand your cloud provider's** security offerings. Ask questions about disaster recovery and data ownership.
- **Review security updates frequently** and take action quickly.

If you suspect you've been targeted:

- **Don't delay.** Acting quickly after an event can minimize damage to your business.
- **Contact your bank's servicing desk** or support staff to report a fraulent transaction as soon as you can.
- **Change all passwords** that cyber criminals may have stolen.
- **Know and follow your local laws** and guidelines for cyber incidents.
- **Document everything** about the event. The more information you have, the better armed you will be to assist an investigation by your company, your bank and law enforcement officials, and the better prepared you will be against future events.

The Growing Threat, Measured

$3.86 million

Average cost of a data breach.[1]

$12.7 billion

Estimated global market for cloud security technologies in 2023.[2,3]

22%

Number of breaches in 2019 that involved cloud assets.[4]

[1] https://www.ibm.com/security/data-breach

[2] https://www.eweek.com/security/cloud-security-spending-set-to-grow-forrester-forecasts

[3] https://www.forrester.com/report/Forrester+Analytics+Cloud+Security+Solutions+Forecast+2018+To+2023+-Global/-/E-RES148715

[4] Verizon DBIR 2019

Be Cyber Secure: Cloud Computing

Why It's Important

Cloud providers use security tools to keep data safe, but some security controls are your responsibility. Without the proper security measures in place, cyber criminals may still be able to access your cloud account.

With access to your account, cyber criminals can:

- **Obtain data** that could be used to steal money or steal your identity.
- **Hold data hostage** with ransomware, a type of malware that encrypts your files and prevents you from accessing them, causing major disruption to your business.
- **Access corporate secrets** to sell data or blackmail the individual or their organization.
- **Get contact information** for your friends and business associates, and phish for their data by getting them to click or download malicious software.
- **Infect key files and data** with viruses, known as malware.

Global Information Security at Bank of America

The GIS team is made up of information security professionals staffing multiple security operations centers across the globe who work 24/7 to keep data and information safe.

For more information, go to:
www.bankofamerica.com/privacy/overview.go