Client Information Security Awareness

BNP Paribas Bank

1. INTRODUCTION

In line with **BNP Paribas**' policies on Internet security, the BNP Paribas portal and its business areas - **BNP Paribas Corporate & Institutional Banking (including BP2S)**, **BNP Paribas Asset Management** and **BNP Paribas Wealth Management** - maintain the highest security standards to avoid fraudulent actions and exposure of confidential data.

Despite these measures the risk related to online banking **cannot be** completely eliminated. This document proposes a number of recommendations to raise client awareness and safeguard online activity. It is recommended that this page be periodically reviewed in order to remain aware of the ever evolving security threats.

2. INTERNET BANKING RISKS

2.1. Malware

Malware, short for malicious software, is software used or programmed by attackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems.

Malware is a general term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, Trojan horses, key-loggers, spyware and other malicious programs.

Fraudsters commonly use Phishing or Social Engineering techniques to install malware on your computer.

2.2. Social Engineering

Social engineering is a term that describes a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures.

The fraudster attempts - by posing as a trustworthy counterparty - to piece together enough information to infiltrate an organization's infrastructure.

Important Information: BNP Paribas will **NEVER** call to solicit your account credentials.

2.3. Phishing

Phishing is a technique of fraudulently obtaining private information. Typically, the fraudster sends an e-mail that appears to be legitimate requesting "verification" of information and warning of some dire consequence if it is not provided. The e-mail usually contains a link to a fraudulent web page that seems genuine - with company logos and content - and requests personal data, which is then used to commit identity theft and/or commit fraudulent actions.

Important Information: It is recommended clients use caution and ensure the website followed via emails is legitimate prior to entering credentials. Fraudsters often lure clients into using their credentials (e.g. logon ID, password, and one-time password (OTP) generated from the security device) on fake web pages.

3. BNP PARIBAS SECURITY PRACTICES

BNP Paribas (the “Firm”) is resolute in protecting its information assets, data, and client information.

This statement summarizes the Firm’s approach to information security. It provides an overview of the measures taken by the Firm to secure client information and ensure confidentiality, integrity and availability of data. The specifics of these measures may vary depending on the services provided.

The Firm endeavors to handle data securely via a defense-in-depth approach, aiming to protect the information assets of the Firm and its clients from unauthorized collection, retention, use, disclosure, modification or destruction. This is approached through appropriate policies, procedures, guidelines and technical security architecture.

The Firm’s information security policy and controls are continually evaluated to ensure relevance and alignment with industry standards/requirements. The Firm’s policies and procedures provide coverage of critical information security areas, including:

3.1. Access Control

Access is granted on a least-privilege and need-to-know basis. All access is granted based on user profiles and with proper prior approval in an Access Right Management platform. Usage of removable media is controlled and forbidden by default.

3.2. Application Security

Prior to implementation, applications are subject to a security certification process to confirm that they have been developed in accordance with our information security policy and secure application

development standards. Regular audits and penetration testing validate the strength of sensitive applications.

3.3. Change Control

The implementations of changes are controlled by the use of a formal change control procedures. Changes required management approval prior to implementation in the production environment.

3.4. Data Availability

The systems and data are backed up in a secure fashion for restoration in case of need. Necessary backup or disaster recovery systems are in place to ensure resilience of systems and data in the event of unforeseen unavailability of the production environment.

3.5. Data Confidentiality

Secure network protocols are used for sensitive traffic and complemented with technical solutions to detect or block the extraction of data. Encryption is employed for data transmissions across public networks and on portable media devices.

3.6. Disaster Recovery

The Firm seeks to protect people, facilities, infrastructure, business processes, applications, and data during and after catastrophic events. The response and system recovery of critical business applications and processes has been carefully planned and tested. The Firm's disaster recovery methodology incorporates the following:

- Business impact analyses.
- Mission-critical disaster recovery plans.
- Regular testing of disaster recovery plans to verify operational readiness.

3.7. Governance

Dedicated security teams cooperate regionally and globally within the BNP Paribas Group. The teams are structured in specialized poles ensuring a permanent coverage of applications, systems, and data security, as well as appropriate response to security incidents. A local CISO oversees the setup, maintains the security policies framework, and seeks to ensure the security strategy is appropriate to cover the security risks appropriate to the operating and regulatory environment.

3.8. Human Resource

The recruitment process includes security screening of individuals prior to onboarding. A security awareness program ensures employees know the risks and can react properly. The security policies enforce employees' duties and responsibilities in regard to the protection of data.

3.9. Incident Response

A regional incident response team manages, controls, and remediates security-related incidents and monitors the effectiveness of controls. Firm security consoles are enriched via vetted and externally source threat intelligence relevant to the threat landscape.

In the event of a breach, the incident response team will promptly take action to secure information and mitigate the breach. Timely notifications of affected clients are issued according to contractual, regulatory, and legislative requirements.

3.10. Network Defense

Network access controls are in place to segregate network segments and filter incoming and outgoing traffic with external parties along with 24/7 monitoring and intrusion detection.

3.11. Physical Security

Physical security measures are in place and designed to provide restricted and recorded access as well as help detect and deter intrusions. Measures are in place to notify physical security personnel of adverse environmental conditions that may affect the electronic communication systems.

3.12. System Defense

Malware protection is installed at all key points of the network and regularly updated to ensure prompt detection and elimination of malicious code. In addition, configuration baselines enforce the deployment of secure systems. A patching program ensures the systems are up-to-date, with a focus on security updates. Regular vulnerability checks ensure that no system was overlooked.

3.13. Threat Intelligence

The firm has established processes for the gathering and analyzing of threats in cyberspace, specifically tailored to the Firm's threat landscape and industry vertical. The Threat Intelligence function stays ahead of cyber actors via timely, accurate, and relevant intelligence.

3.14. Vendor Management

The Firm's Vendor Management Program conducts due diligence on third-party activities related to information security, procurement, contracts, data privacy, including:

- Evaluation of prospective vendors for compliance with the Firm's policies and controls.
- Due diligence reviews, including preparation of risk ratings and findings.
- Mitigation of risk findings.
- Support in vendor selection and contract negotiations.

3.15. Vulnerability Management

The Firm's Security Operations Vulnerability Management Team, in charge of vulnerability management, scans and analyzes information assets. Mitigating controls are enforced where needed and the patching program deployed with prioritization of critical assets.

4. CLIENT RECOMMENDATIONS

In order to avoid fraudulent actions and exposure of confidential data, BNP Paribas recommends its clients to take a number of guidelines into account related to workflow management and the protection of the their infrastructure summarized in 10 recommendations.

4.1. RECO 1 - Implement 4-eyes Principle

Respect the 4-eyes principle for all key services like entitlements management, payment authorization, and beneficiary management

4.2. RECO 2 - Review User Access

IT admin must review user access at least once a year

4.3. RECO 3 - Use Up-to-date Software Versions

Software includes operating systems (e.g. Microsoft Windows), browsers (e.g. Internet Explorer, Firefox, Chrome) and other critical software (e.g. Java, Flash, Antivirus, Firewall and Anti-Spyware)

4.4. RECO 4 - Keep Personal Information Private

Tokens and passwords are personal and can never be disclosed to anyone. It is of utmost importance that login credentials are secured as these constitute the entry-points to BNP Paribas platforms. The following guidelines can assist in keeping your private information safe:

- Avoid reusing the same usernames and passwords that you use for other website logins
- Do not use information that can be easily deduced
- Even though your user ID (usually the email address) itself is not confidential, do not write it down on anything that can be easily found by a malicious person.
- Never write down or reveal your password, SecureID Serial or pin number to anyone, including BNP Paribas Support Teams
- Change your password periodically
- Ensure that you are not being observed when entering your password
- Periodically check your keyboard and computer to ensure that no key loggers (devices that record keystrokes) are maliciously connected
- Many browsers contain auto-complete functionality. Whilst this saves time for the user, it also allows unauthorized individuals to log into your account if your computer remains unlocked and unattended. BNP Paribas recommend that you disable your web browser's auto-complete functionality.
- Whatever the circumstances never communicate your PIN/secret code to anyone (including BNP Paribas support teams) and make sure nobody knows it.

Authentication Devices:

- Should you be issued with authentication tokens or one-time passwords sent to mobile device, please ensure that these devices are kept secure at all times.
- Do not communicate by phone or to an unknown email address the serial number written behind the token, even if claiming to be from a support team, unless yourself have contacted a relevant support team earlier for a PIN reset or card synchronization issue. In that later case, it is OK to communicate the serial number to BNP Paribas Client Service Desk for action.
- In any case, do not paste or write anything on the SecurID token!
- Last but not least, if you lose or believe you could have lost your token, please contact BNP Paribas Client Service Desk as soon as possible so that we can disable your token.

4.5. RECO 5 - Protect Your Workstation against Hacking and Malware

Protect your computer from hackers, viruses and malicious program.

Antivirus software, anti-spyware software, and personal firewalls should be installed and continually kept active on your computer. Security patches and virus definitions should be periodically installed and updated in order to ensure that any bugs and security loopholes are closed.

Perform Antivirus and Anti-Spybot scans on a regular basis. If your antivirus or antispyware program detects a suspicious file, immediately delete said file and close the website that has downloaded that file. If the computer has been compromise, do not hesitate to change all your passwords.

Do not conduct any transactions through public or shared computers.

4.6. RECO 6 – Do Not Leave Your Workstation Unattended

Do not leave workstations unattended when logged-in and always remember to log-off when e-banking transactions have been completed.

It is highly recommended that browser applications are closed fully after using any BNP Paribas platforms.

4.7. RECO 7 - Only Visit Trusted Websites

Only visit trusted websites and do not download any files or programs from unknown or suspicious websites. Always be careful when opening an unknown file, a strange e-mail or a new program or when clicking certain links.

4.8. RECO 8 – Beware of Fraudulent Emails and Websites Claiming to be BNP PARIBAS

Remain vigilant for suspicious emails and websites that attempt to use deceit in order to reveal sensitive information. BNP Paribas will never ask you for private information by email and will not send e-mails with embedded hyperlinks to transactional websites.

Always verify that the email sender is trustable before opening any attachment, and do not respond or click on any links provided in e-mail messages that appear to be sent by BNPP, asking you to enter personal data, bank account / card numbers or Internet Banking codes.

Also, please be aware that in some email applications such as Microsoft Outlook, a text hyperlink may be displayed but actually clicking on the hyperlink may direct you to another website. This is known as phishing. Phishing websites are designed to look identical to genuine websites. Additionally, some emails may contain image files that appear to look like text. Hovering over the image and clicking may lead you to a phishing website. Ensure that the guidelines for verifying BNP Paribas websites (above) are followed.

Navigating to the BNP Paribas website should always be done through known hyperlinks. Please read the address bar/URL carefully and always ensure that the domain is the expect one. Another method of verifying the authenticity of the BNP Paribas website is to check the digital certificate for websites that begin with "**HTTPS**". Certification Authorities (such as Verisign or Geotrust) are trusted third party

issuers of digital certificates which verify that the website URL is a genuine site of the company or business in question. Click on the padlock next to the URL to see details of the Certification Authority.

4.9. RECO 9 - Do Not Act On Suspicious Calls from BNP PARIBAS

If someone calls you up, pretending to work for or to act on behalf of BNP Paribas, and asks you to provide personal data and/or initiate/authorize transactions, refrain from taking any action at all and contact your L1 Support entry point (See **RECO 10**).

4.10. RECO 10 - In Case Of Doubt, Contact BNP PARIBAS

Immediately abort any transaction and take contact with BNP Paribas in case of doubt, especially when the procedure for signing differs from the usual procedure. It is advised to check whether or not all on-going transactions are legitimate. Please contact your Support entry point in case of doubt.

Should you suspect any unauthorized access or have any outstanding queries regarding Information Security, please promptly contact your relationship manager or support team on mail Latam.CSIRT@bnpparibas.com.

5. DISCLAIMER

This document has been prepared by **BNP PARIBAS** for informational purposes only. Although the information in this document has been obtained from sources which **BNP PARIBAS** believes to be reliable, it shall not constitute any representation, warranty, assurance, guarantee or inducement by the Firm as to the adequacy, accuracy or sufficiency of the measures described herein for any contemplated purposes. Such information may be incomplete or condensed.

This document does not constitute a prospectus or solicitation. All estimates and opinions included in this document constitute our judgment as of the date of the document and may be subject to change without notice. Changes to assumptions may have a material impact on any recommendations made herein.