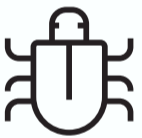


ONLINE BANKING SECURITY AWARENESS

“The following information proposes a number of recommendations to raise your awareness and safeguard your online activity. It is recommended that this document be periodically reviewed in order to remain aware of ever evolving security threats.

Internet Banking Risks



Malware

Malware, short for malicious software, is a 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 can use Phishing or Social Engineering techniques to install malware on your computer.



Phishing

Phishing is a form of social engineering, with the goal of fraudulently obtaining sensitive confidential information. Phishing e-mails typically include one or more of the following characteristics: appear to be from a legitimate sender; the email subject conveys an important message; the content of the email may promise a benefit to the recipient, or request a time-sensitive reply and can establish consequences for non-adherence; and may ask the recipient to click a link or download an attachment. The e-mail can contain a link that launches an attack, or a link that takes the recipient to a fraudulent website or a corrupted file attachment.



It is recommended that you use caution and only click on links to trusted websites, do not open email attachments that seem suspicious, and do not provide sensitive information to unknown websites. 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.



Social engineering is a term that describes a non-technical kind of intrusion that relies heavily on human interaction and often involves manipulating human behavior to break established security measures. Typically, a fraudster – will pose as a trustworthy counterparty to extract confidential information from an employee that will allow access to an organization’s infrastructure, using a well-mastered scenario, such as:

Social Engineering



Fake CEO scam:

Phone calls and/or emails from an individual claiming to be part of your company’s Senior Management, requesting an urgent and confidential transfer of a large sum of money for very secretive reasons (e.g. a take-over, tax reasons or a large confidential transaction).




Fake vendor scam:

Phone calls and/or emails from an individual impersonating your supplier, notifying of a change in bank account details, and requesting to make future payments into a fraudulent account.



Fake technician scam:

Phone calls from an individual impersonating your bank service desk or your software vendor, pretexting a migration, a test, an upgrade... of your e-banking system. The fraudster generally asks you to allow him to remotely access your workstation, which allows him to make fraudulent transfers.

 BNP Paribas will never call to solicit your account credentials. If you are contacted to provide account credentials, do not provide them.

BNP Paribas Security Practices

BNP Paribas is resolute in protecting its information assets, data, and client information.

The BNP Paribas endeavors to handle data securely via a defense-in-depth approach, aiming to protect the information assets of the BNP Paribas 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 BNP Paribas’s information security policy and controls are continually evaluated to ensure relevance and alignment with industry standards, and regulatory requirements. The BNP Paribas’s policies and procedures provide coverage of critical information security areas, including:

Access Control



System and platform 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.

Application Security



Applications are subject to a security certification process in accordance with the BNP Paribas’s Information Security Policy and secure application development standards. Regular audits and penetration testing validate the strength of sensitive applications.

Change Control



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

Data Availability



BNP Paribas 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.

Data Confidentiality



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

Disaster Recovery



The BNP Paribas has implemented policies and procedures to protect people, facilities, infrastructure, business processes, applications, and data before, during, and after catastrophic events. The response and system recovery of critical business applications and processes have been carefully planned and tested. The BNP Paribas’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

Governance



Dedicated security teams cooperate locally, 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 (Chief Operating Security Officer) oversees the setup, maintains the security policies framework, and seeks to ensure the security strategy is appropriate to cover the security risks applicable to the operating and regulatory environment.

Physical Security



Physical security measures are in place and designed to provide restricted and recorded access as well as detect and deter intrusions.

Measures are in place to notify physical security personnel of adverse environmental conditions that may affect the electronic communication systems.

Vendor Management



The BNP Paribas's Vendor Management Program conducts due diligence on third-party activities including, but not limited to information security, procurement and data privacy, including:

- ✓ Evaluation of prospective vendors for compliance with the BNP Paribas's policies and controls.
- ✓ Due diligence reviews, including preparation of risk ratings and findings.
- ✓ Mitigation of risk findings.

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. BNP Paribas security policies enforce employees' duties and responsibilities in regard to the protection of data.

Network Defense



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

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 consistent deployment of secure systems. A patching program ensures BNP Paribas system protections are up-to-date, with a focus on security updates. Regular vulnerability checks ensure that no system was overlooked.

Vulnerability Management



The BNP Paribas's Security Operations Vulnerability Management Team is in charge of vulnerability management, and conducts scans to analyze information assets.

Mitigating controls are enforced where needed and the patching program deployed with critical assets prioritized.

Incident Response



A regional incident response team manages, controls, and remediates security-related incidents and monitors the effectiveness of controls. The BNP Paribas has a threat intelligence service, which updates and enriches its security consoles via vetted, externally sourced threat intelligence. The BNP Paribas's defenses are on the lookout for any known cyber threats.

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

Threat Intelligence



The BNP Paribas has established processes for the collection and analysis of threats in cyberspace, specifically tailored to the BNP Paribas's threat landscape and industry vertical.

The Threat Intelligence function seeks to stay ahead of cyber actors via timely, accurate, and relevant intelligence.

Certifications



As part of its commitment to quality and security, BNP Paribas has sought certification for the key processes related to the exploitation and development of the Connexis Cash platform:

ISO:9001 certified - standard for quality management, granted to exploitation and infrastructure of Connexis Cash platform

ISO:20000 certified - standard for IT service management, granted to exploitation and infrastructure of Connexis Cash platform

ISO:27001 certified - standard for information security management, granted to exploitation and infrastructure of Connexis Cash platform and also to development and management of the Connexis Cash platform itself.

Recommendations

In order to help avoid fraudulent actions and exposure of confidential data, the BNP Paribas recommends you take note of the following 10 recommendations related to workflow management and the protection of infrastructure:

1 Implement the 4-Eyes Principle

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

2 Review User Access

IT administrators should review user access at least once per year.

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). Software and patches should routinely be updated.

4 Keep Personal Information Private

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

- ✓ Do not duplicate the same usernames and passwords that you use for other website logins, whether personal or work-related;
- ✓ Do not use information that can be easily deduced, like date of birth or phone number;
- ✓ 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 any digital password, SecurID 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. The BNP Paribas recommends that you disable your web browser's auto-complete functionality.
- ✓ **Whatever the circumstances, never communicate your PIN/secret code to anyone (including the BNP Paribas's support teams) and make sure no one except you knows it.**



Authentication Devices:

- ✓ Should you be issued an authentication token or one-time password sent to a 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, you can communicate the serial number to BNP Paribas Client Service Desk for action.
- ✓ In any case, do not paste or write anything on the SecureID token.
- ✓ If you lose or believe you may have lost your token, please contact BNP Paribas Client Service Desk as soon as possible so that we can disable your token.

Your Personal Information:

Please keep the BNP Paribas updated with accurate details of your personal information.



5 Protect Your Workstation Against Hacking And Malware

There are ways to protect your computer from hackers, viruses and malicious programs.

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 installed and routinely 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 compromised, immediately change all your passwords.

Do not conduct any BNP Paribas transactions through public or shared computers.



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.



7 Only Visit Trusted Websites

Only visit trusted websites and do not download any files or programs from unknown or suspicious websites. Always validate the source when opening an unknown file, a strange e-mail or a new program, and never click on suspicious links.



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 steal sensitive information. The 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 trusted before opening any attachment, and do not respond or click on any links provided in e-mail messages that appear to be sent by the BNP Paribas, asking you to enter personal data, bank account / card numbers or Internet Banking codes.



9 Do Not Act On Suspicious Calls from BNP PARIBAS

If someone calls you claiming 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 immediately contact the BNP Paribas Client Service Desk.



10 In Case Of Doubt, Contact BNP PARIBAS

Immediately abort any transaction and contact BNP Paribas in case of doubt, especially when the procedure for signing differs from the standard established procedure. It is advised to check whether or not all on-going transactions are legitimate. Please contact the BNP Paribas Client Service Desk.

Should you suspect any unauthorized access or have any outstanding queries regarding Information Security, please promptly contact your relationship manager or the BNP Paribas Client Service Desk.

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 can be a cyber-attack known as phishing, and described above. 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 (below) are followed.

Navigating to the BNP Paribas websites should always be done through known hyperlinks. Please read the address bar/URL carefully and always ensure that the domain is the correct one. The BNP Paribas websites are secure sites, indicated by the address beginning with "https". The 's' at the end of https means communications between the web browser and the website you are using are encrypted. 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. You are able to click on the padlock next to the URL to see details of the Certification Authority.

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 BNP Paribas 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 or legal advice. 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.

You are solely responsible for (a) maintaining the security of your devices used for accessing BNP Paribas websites, and (b) for the confidentiality of your user account information, including your access credentials. You are solely responsible for any and all activity that occurs on your user account as a result of your sharing this information or failing to keep this information secure and confidential, except as otherwise provided by law.

This document may not be reproduced (in whole or in part) to any other person without the prior written permission of BNP Paribas.

© 2019 BNP PARIBAS. All rights reserved.