Deutsche Bank

Cyber Fraud Prevention

At a glance
How to prevent cyber fraud

Reduce to the essentials

Install only what you need

- Keep what is installed up to date
- If you do not need something, uninstall it

Spam/Phishing

- Delete spam from unknown senders immediately
- Check links (text/images) – do not click on file attachments in suspicious e-mails
- If in doubt, forward suspicious emails to your IT Security department

CEO-Fraud

- Challenge payment orders to unknown bank accounts
- Always contact your CEO via contact details which are available in your company address book
- Always check the credibility and plausibility of the information provided

Approval of payments

- Clear demarcation of duties
- Only use the dual control principle
- Two-factor authentication
- Even if put under great pressure, do not trust blindly

Password protection

- Use different and complex passwords for different systems
- Delete inactive accounts
- Install latest security updates/anti-virus protection
- Set macro settings to a high level

Awareness of employees

- Implement cyber security training sessions
- Newsletter and tests on social engineering fraud & phishing

Definitions of attack types

Types of common attacks

- Phishing
  Bogus emails that trick users into supplying confidential information such as user IDs and passwords
- Smishing
  Phishing by SMS messaging. A text message is sent to an individual's mobile phone requesting personal information under false pretences
- Vishing
  So-called "war dialers" call thousands of numbers at a specific time. When a call is answered, an automated recording claims that a credit card or bank account has been compromised, and request the targeted individual to supply personal information.
- Spear Phishing
  Targets high profile individuals (CFOs, CIOs) within an enterprise to obtain confidential information
- Trojan attacks
  Use of malicious software that appears to perform a specific function for the user, but instead facilitates unauthorised access to their computer system or encrypts all data (Locky)
- "Man-in-the-browser" attacks
  These intercept data using a secure communication between a user and an online application. The Trojan embeds in the browser application, and can intercept and manipulate any information that a user submits. Trojans are also being used to attack instant messaging applications.
- Viruses
  These are spread via ad-related spam email
- Key logger robot
  Programmes that record keyboard keystrokes to collect user access IDs and account information
- Social engineering
  Rogue phone calls, emails or other type of manipulation of people forcing them into performing actions or divulging confidential information

Methods of attack

Internet fraud and cybercrime schemes

The Business email Compromise (BEC) is rapidly becoming the most commonly-used method of attack by cyber criminals where scams target businesses that regularly perform wire transfers.

"Fake President"

- Email account of a high-level executive within a company (usually the CEO or CFO) is exploited
- Fake email is sent to the company's controller requesting a significant amount is wired to a foreign bank account
- Fraudulent email asks the transfer be executed on an urgent basis to facilitate a foreign transaction

Employee's personal email hacked

- An employee of a business has his/her personal email hacked
- Requests for invoice payments to fraudster-controlled bank accounts are sent from this employee's personal email to multiple vendors identified from the employee's contact list
- The businesses may not become aware of the fraudulent requests until they are contacted by their vendors to follow-up on the status of the invoice payment

Phishing email with fake links

- A criminal sends an email to a payment operations employee in the targeted corporation. These emails appear to be from the financial provider asking you to update your payment system software
- The phishing email will ask you to fill out a form or click on a link or button that takes you to a fraudulent website. The fraudulent website mimics the company referenced in the email, and aims to extract your personal data including user ID and password from the targeted online banking application

Best practices to mitigate internet payment fraud

Email account protection

- **Delete spam**
  Immediately delete unsolicited email (spam) from unknown parties

  Do not open spam email, click on links in the email, or open attachments

  These often contain malware that will give criminals access to your computer system
- **"Forward" vs. "Reply"**
  Do not use the "Reply" option to respond to any business emails

  Instead, use the "Forward" option and either type in the correct email address or select it from the email address book to ensure the intended recipient's correct email address is used
- **Check all requests with a false sense of urgency**
  Many spam emails tell you that your account will be in jeopardy if something critical is not updated right away

  Also be alert if you receive an urgent email from your CEO or CFO asking you to execute a confidential transaction within a short period

  Always call back the CEO or CFO for verification
- **Check emails requiring system upgrades**
  Always contact your bank relationship manager when you receive an email requesting you to upgrade your online banking application

Employee awareness

- Establish cyber security awareness training for all employees
- Distribute regular newsletters with the latest fraud trends and protection advisory
- Execute social engineering fraud rehearsals

Computer security

- Avoid downloading programmes from unknown sources including internet and USB sticks
- Ensure your computer has the latest malware protection
- Keep anti-virus software installed and updated
- Ensure you have the latest security updates installed on your computer, and consider using high-level macro security settings in software applications
- Consider using a separate computer dedicated to making online payments with special physical security controls
- Do not use the same password for different systems, change them regularly and delete inactive accounts

Best practices to mitigate internet payment fraud

Payment execution protection

- Dual approval-joint account
  All payment execution should request dual system-enforced approval above a certain limit
- Two-factor authentication for payment release
  Payment authorisation should always require two-factor authentication, based on a physical or software app token
- Monitor and reconcile payment accounts daily
- Implement out of the band transaction notification
  For high volume/amount wires, request out of the band transaction initiation notifications
- Two-factor authentication for client login
  Where possible, use two-factor authentication for client login
- Payment account white list
  Maintain a white list of valid payment accounts authorised to receive payments. Changes to the white list should be validated via a dual control
- Segregation of duties
  Ensure proper segregation of duties between payment creation, payment approval and payment release
- HR policy
  Ensure that job rotation and forced vacation are implemented for payment officers

Information Security @ Deutsche Bank

- One of our top priorities is to protect the confidentiality, integrity and availability of customer data and the Bank's information assets
- Deutsche Bank has established a comprehensive information and cyber security programme that includes:
  - Codified security policies and standards, updated on a regular basis (including on IT vendors)
  - Physical (access controls, secure data centres), technical (authentication and authorization, network zoning) and administrative controls (segregation of duties, neutral controls, regular staff recertification)
  - The latest security technology, including anti-malware, encryption, network intrusion detection, security patching
  - The implementation of an industry-leading third party solution for the detection and mitigation of Distributed Denial of Service (DDoS) attacks
- Deutsche Bank's security professionals are keeping up-to-date with cyber security threats and the latest protection, detection and response solutions, by closely collaborating with external security experts from security vendors, research groups and other companies. We also attend industry standard security training and conferences
- Deutsche Bank's Cyber Intelligence team subscribes to threat intelligence services and actively shares anonymised information with industry partners and groups such as the FS-ISAC (Financial Services-Information Sharing and Analysis Center)

Information Security @ Deutsche Bank

- External vulnerability scanning and internal device scanning are conducted to identify and close potential cyber security vulnerabilities. All Internet-facing applications are regularly tested by industry experts to allow secure execution
- The compliance of IT systems with Deutsche Bank's security policies and standards is continuously monitored, and tested in Red Team exercises (a dedicated team viewing Deutsche Bank's assets from an adversarial perspective with the goal to understand likely hacker techniques and better prepare against an attack)
- 24x7 security monitoring of Deutsche Bank's critical IT systems
- 24x7 global security hotline for all employees and service providers, to report cyber security related issues, are in place to detect anomalies and potential security breaches
- Mandatory information security training and awareness courses for internal and external staff are regularly conducted, and tracked for completion. To complement training, other channels are utilised to convey awareness, including a dedicated website, videos, phishing campaigns and cyber security roadshows.

Contact us.

For further information, please contact your relationship manager or product specialist.

Email: gtb.marketing@db.com
Internet: http//cib.db.com/