Cyber Fraud Prevention

December 2016

Passion to Perform
Agenda

- Information Security @ Deutsche Bank
- Definitions of different attack types
- Internet fraud and cyber crime schemes
- Best practices to mitigate internet payment fraud
- Internet security resources
Information Security @ Deutsche Bank – Overview (1/2)

- One of Deutsche Bank AG and its group member’s (“Deutsche Bank”) highest 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 program with a high standard financial industry security governance framework and organization to implement control and adherence to security policies and standards in conjunction with evolving business requirements, regulatory guidance and an emerging threat landscape.

- Deutsche Bank’s security policies and standards are codified and updated on a regular basis. In addition, Deutsche Bank’s IT vendors have to comply with the bank’s policies and standards and are subject to Deutsche Bank’s risk assessments and periodic vendor control assessments.

- Physical (e.g. access controls, secure data centres), technical (e.g. authentication and authorization, network zoning) and administrative controls (e.g. segregation of duties, neutral controls, regular staff recertification) are in place to proactively mitigate the risk of unauthorized access and manipulations at network, system, application and database level and support data processing standards in line with legal data protection requirements.

- Latest security technology, e.g. anti-malware, encryption, network intrusion detection, security patching, as well as a dedicated data leakage prevention (DLP) program, is used to protect customer data and Deutsche Bank’s information assets, systems and services. In addition, Deutsche Bank has implemented 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 the evolving cyber security threat landscape and the latest protection, detection and response solutions by closely collaborating with external security experts from security vendors, research groups and other companies, as well as by attending industry standard security trainings and conferences. The bank’s Cyber Intelligence Team is subscribed to threat intelligence services and actively shares anonymized information with industry partners and groups, e.g. the FS-ISAC (Financial Services - Information Sharing and Analysis Center). Deutsche Bank’s Head of Cyber Security is a board member of the FS-ISAC.

External vulnerability scanning and internal device scanning is conducted to proactively identify and close potential cyber security vulnerabilities. All Internet-facing applications are tested by industry experts to allow secure execution. In addition, the compliance of IT systems with Deutsche Bank’s security policies and standards is continuously monitored and tested in Red Team exercises.

24x7 security monitoring of the bank’s critical IT systems, as well as a 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.

In order to effectively respond to potential cyber security incidents, a global cyber security response process is operational 24x7. In case of an incident, fast and effective countermeasures will be taken and the remediation of the underlying root causes initiated.

Mandatory Information Security Training & Awareness courses for internal and external staff are regularly conducted and tracked for completion. To complement training, other channels are utilized to convey awareness, including a dedicated website, awareness videos, phishing campaigns, and cyber security roadshows.
Definitions of different attack types

**Types**

- **Phishing**
  Bogus e-mails 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 dial 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.

- **Business**
  Executive Scam:
  Targets high profile individuals (CFOs, CIOs) within an enterprise to obtain confidential information.

**Other common attacks**

- **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.

- **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 user submits. Trojans are also being used to attack instant messaging applications.

- **Viruses**
  These are spread via ad-related spam e-mail.

- **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.
Internet fraud and cybercrime schemes

The Business e-mail Compromise (BEC) is rapidly becoming the most commonly used method of attack by cyber criminals where scams target businesses that regularly perform wire transfer in businesses:

Scheme 1: Business executive scam
- 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 wire be executed on an urgent basis to facilitate a foreign transaction.

Scheme 2: Bogus invoice scheme
- Fraudsters email a business with an invoice purporting to be from a regular supplier or trusted source.
- The invoice appear a normal looking document, but to view the file, the recipient has to enable a macro which installs malware into the computer.
- The malware will then log the company’s online banking credentials, along with other financial information, before sending it back to the criminal. The data is then used to steal money from the bank account of the business.
Internet fraud and cybercrime schemes

Scheme 3: Employee personal email hacked
- An employee of a business has his/her personal e-mail hacked.
- Requests for invoice payments to fraudster-controlled bank accounts are sent from this employee’s personal e-mail to multiple vendors identified from the employee’s contact list.
- The business 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.

Scheme 4: 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 informing about an update on payment system software.
- The phishing email will ask you to fill-out a form or click on a link or button that take 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.

Scheme 5: Rogue phone calls
- A fraudster phones in (either as “hotline”, with the “need” to ensure proper functioning and asking for one time passwords, which is then followed up by a email with the fake account details, to lure the company to transfer money to an incorrect account).
Best practices to mitigate internet payment fraud

Email account protection

Delete spam
- Immediately delete unsolicited e-mail (spam) from unknown parties.
- Do NOT open spam e-mail, click on links in the e-mail, 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 e-mails.
- Instead, use the “Forward” option and either type in the correct e-mail address or select it from the e-mail address book to ensure the intended recipient’s correct e-mail address is used.

Check all requests with a false sense of urgency
- Many scam 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 you 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.
# 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 always should 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**
  When possible use two factor authentication for client-login.

- **Payment account white list**
  Maintain a white list of valid payment accounts that are the only 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 force vacation is implemented for payment officers.
# Best practices to mitigate internet payment fraud

## Computer security
- Avoid downloading programs 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.

## Employee awareness
- Establish cyber security awareness training for all employees.
- Distribute regular news letters with the latest fraud trends and protection advisory.
- Execute social engineering fraud rehearsals.
Internet security resources

Latest cyber security advisory news can be found at:

- The Internet Crime Complaint Center
  www.ic3.gov
- The Financial Fraud Action
  www.financialfraudaction.org.uk
- International Information Systems Security Certifications Consortium
  www.isc2.org
- Stop Fraud
  http://www.stopfraud.gov/
- Financial Services Sharing Information Center
  https://www.fsisac.com/
- Allianz für Cyber-Sicherheit
  www.allianz-fuer-cybersicherheit.de
- US CERT
  https://www.us-cert.gov/
Disclaimer

This presentation is for information purposes only and is designed to serve as a general overview regarding the services of Deutsche Bank AG, any of its branches and affiliates. The general description in this presentation relates to services offered by Global Transaction Banking of Deutsche Bank AG, any of its branches and affiliates to customers as of June 2015, which may be subject to change in the future. This presentation and the general description of the services are in their nature only illustrative, do neither explicitly nor implicitly make an offer and therefore do not contain or cannot result in any contractual or non-contractual obligation or liability of Deutsche Bank AG, any of its branches or affiliates.

Deutsche Bank AG is authorised under German Banking Law (competent authority: German Banking Supervision Authority (BaFin)) and, in the United Kingdom, by the Prudential Regulation Authority. It is subject to supervision by the European Central Bank and by BaFin, Germany’s Federal Financial Supervisory Authority, and is subject to limited regulation in the United Kingdom by the Prudential Regulation Authority and Financial Conduct Authority. Details about the extent of our authorization and regulation by the Prudential Regulation Authority and regulation by the Financial Conduct Authority are available on request.

(Copyright© December 2016) Deutsche Bank AG. All rights reserved."