Deutsche Bank
Global Transaction Banking

# The Lexicon of cyber-crime: Definitions of attack types

As business becomes more technology-oriented and innovative new products and solutions emerge on a regular basis, criminals also rise to the challenge of breaching firewalls and technology designed to protect companies from cyber-crime. At the same time, criminals also aim to catch their victims unaware, attempting to mislead them into revealing confidential information. These are the most common forms of attack:

## Phishing

This usually manifests itself in the form of bogus emails that trick users into supplying confidential information such as user IDs and passwords. A derivative of phishing is 'Spear Phishing' which targets high profile individuals such as CEOs, CFOs and CIOSs and attempts to send emails from a trusted sender to individuals/groups, with the aim of extracting confidential information by deception.

This is how it works. A criminal sends an email to a payment operations employee in the targeted corporation. These emails appear to be from the financial provider requesting an update of payment system software. The phishing email will request that a form is completed or will include a link that takes the unsuspecting victim to a fraudulent website. This website mimics the company reference in the email and aims to extract personal data including user ID and password from the online banking application.

## Smishing

This is, effectively, phishing by SMS messaging. A text message is sent to an individual's mobile phone requesting personal information under false pretences. This activity often preys on people's panic or sense of urgency, notably if the criminal is posing as a bank or other financial institution.

## Social engineering

Rogue phone calls or emails or other types of manipulation of people forcing them into performing actions or divulging confidential information.

## Vishing

This is the criminal practice of using social engineering over the telephone to gain access to private personal and financial information. It involves a phone call and an automated message claiming that a credit card or bank account has been compromised and requests personal information from the victim. A variation of vishing is the rogue telephone call that requests information.

## Trojan attacks

Many of these are spread by some form of social engineering, either by a misleading email with an attachment or by a drive-by download. Invariably, ransomware attacks are often carried out by Trojans. It involves use of malicious software that appears to perform a specific task but in fact facilitates unauthorised access to someone's computer system or encryption of data. The so-called 'man-in-the-browser' attacks are also a form of Trojan. 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 a user sends. Trojans are also being used to attack instant messaging applications.

## Viruses

These are varied and many are spread via ad-related spam emails.

## Key logger robots

These programmes record keyboard keystrokes to collect user access IDs and account information.

## Email hacking

The email of an employee of a business is hacked and fraudulent activity takes place which goes undetected for a period of time. Email hacking can also include violation of a high-level executive's account with fake instructions being sent out requesting cash transfers.

## CEO fraud

An email account of a high level executive is exploited, with a fake email being sent to instruct the transfer of significant sums of money to a designated [often foreign] account.

## Ransomware

Malware programmes used by hackers to block, access or use of data or an entire computer system. The aim is to encrypt the data and then extort money for unlocking the data.

## Invoice redirection fraud

Cyber-criminals access the correct payment information and account details of a supplier/ customer, then try to change the details to redirect sums of money to their own account (s).

# Checklist:
## How to prevent cyber fraud

### Audience awareness
- Implement cyber-security training
- Socialise changes and updates

### Keep it simple
- Install on your computer only what you need
- Maintain installations to ensure they are up-to-date
- Uninstall anything you do not need

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

### Question it…
- Challenge payment orders to unknown bank accounts
- Always contact your CEO or other senior figure via contact details available in your company address book
- Always check the credibility and plausibility of the information provided

### Be stubbornly insistent
- There should be clear demarcation of staff duties
- Only use the dual control principle
- Implement two-factor authentication
- Do not trust blindly – even in times of intense activity

### Make it hard for the attackers
- 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

## Recommended further reading

'Combatting cybercrime'
*by Brendan Goode (October 2017)*

'Cyber Security – You are the target!'
*(Deutsche Bank portal, January 2018)*

Third-party risks: the cyber dimension
*(Deutsche Bank/EIU Intelligence Unit, October 2017)*

This article is from www.db.com/flow.
To ensure you don't miss out on regular updates and articles, please share your preferences with us now (and this is a genuine request, and not a phishing ploy!). Here is the registration page