

Security Advisory:

Trojans/Malware

As a result of heightened Trojan/Malware activity targeting business banking customers BPFi is issuing this important advisory.

Publication by:

Banking & Payments Federation Ireland (BPFi)

For the attention of:

Business Institutions and Associations – for onward transmission to their members.


Purpose of Advisory:

The purpose of this note is to make customers aware of Trojans/Malware activity and to implement safeguards in order to protect themselves.

Key Points: For business/corporate banking.

1. There has been heightened activity from new Trojans / Malware variants attacking primarily business banking customers across Europe.
2. Malware is delivered via an email attachment or a link to infected web site.
3. Malware can also be disguised as a pdf, a word file or even a powerpoint file.
4. Once the attachment is opened, the machine is infected with keyloggers and remote access Trojans.

Ways customers can protect themselves - Action:

- Keep your PC's patching up to date.
 - Run a recognised anti - Virus (AV) and anti - malware programme and ensure it is up to date and actively scanning.
 - We advise to carry out your own virus check before opening any attachment.
 - We recommend switching on heuristic scanning option if available.
 - Change passwords regularly.
 - On online business banking review your beneficiary lists and account numbers regularly.
- 

- Ensure that transaction limits are set at a value threshold equal to or just above your regular payment amount.

Always remember: Your bank will never send you an e-mail requesting your bank security details.

This is a general notice issued by the Financial Crime and Security Department of the BPF on Behalf of BPF members.

Disclaimer Note: The information contained in this advisory is for general guidance and for information purposes only and is intended to enhance awareness and vigilance regarding this

