

Cyber methods used for low-tech crime

A British trade association, the Corporate IT Forum, has warned that thieves can use “out of office” auto-replies to target those who are on vacation and burglarize their homes.

In a meeting of the association it was revealed that criminals are buying SPAM e-mail address lists and sending mass e-mail messages with the intention of receiving “out of office” auto-replies containing details of the recipients’ vacation absences. By cross-referencing those names with publicly available personal information, they are able to target empty homes.

“You wouldn’t go on holiday with a note pinned to your door saying who you were, how long you were away for and when you were coming back, so why would you put this in an e-mail?” asked David Roberts, chief executive of the Corporate IT Forum. The Justice Department and the FBI recently stated they had no current investigations of such crimes under way, but were watching for this activity.

To avoid falling victim to this SPAM scam:

What to do...

- Keep messages as bland as possible.
- Redirect inquiries to a colleague’s business phone number so someone can assess the inquiry.
- If you have an important-sounding job title, think carefully about whether you want to reveal it to a wide audience.
- Be careful about giving away alternative contact details; only include them if the person concerned has agreed.
- Always prepare for your absence and warn key contacts personally of your absence.

What *not* to do...

- Never say you are away on vacation, out of town or away from the office between certain dates.
- Never put alternative personal contact details on an “away from office” message.
- Never put your home address, home phone number or personal cell-phone number on the message.
- Never put a colleague’s personal contact details in a message.
- Never use an “away” auto-reply message on your home or personal e-mail. ■