Fraud Protection: Best Practices

Protecting your credentials and accounts online

Source: *Internet Security Threat Report 2014*, Symantec Corporation

Online "account takeover" fraud is the attempt to obtain confidential information — including passwords, personal ID numbers, and token codes — and use it to access your accounts and transfer money or commit other fraudulent acts.

This type of fraud is particularly dangerous because it's often difficult to detect. You may be unaware information has been stolen until the money is gone from vour account.

The primary methods of account takeover fraud are manipulating victims into divulging confidential information, installing malicious software (malware) on a computer without the user's consent, or some combination of these.

You can help protect the cash in your company's accounts with these best practices and effective bank services:

- Implement dual custody — and use it properly.
  - Require all payments or user modifications initiated by one user be approved by a second user on a *different device*.
  - For dual custody to work as intended, both the wire initiator and approver must pay close attention to the wire details — not just give them a rubber stamp. The best practice for initiators and approvers: Verify before you initiate. Verify before you approve.
- Update all your antivirus programs.
- Be cautious of unexpected token prompts or on-screen messaging within your *Commercial Electronic Office*® (*CEO*®) portal session.
  - The *CEO* portal does not prompt for a token during sign on. Users are prompted for a token only when attempting to access high-risk payment services (such as Wires, ACH or Foreign Exchange) and when accessing administrative functions within the *CEO* portal. If you receive a request to enter your token code at any other point during your *CEO* portal session, contact your Treasury Management representative *immediately*.
- Generate transactions from stand-alone PCs on which email and web browsing are disabled.
- Never give out your online banking access credentials. Instruct employees to follow the same rule.
- Don't click on links in emails or text messages, and don't download attachments or install programs, unless you're certain they're from a trusted sender.
- Be wary of unsolicited phone calls from individuals who identify themselves as a Wells Fargo employee calling to help you with an unreported system issue. If you receive a call like this, do not follow the caller's instructions. Immediately contact your Wells Fargo bank representative.
- Monitor online accounts daily to detect suspicious activity.
- Use notification and alert services to receive text or email notifications informing you of electronic debits from your accounts.

For more information, contact your Wells Fargo Dealer Services representative or call 1-888-937-9997, Monday through Friday, 5:00 a.m. to 7:00 p.m. Pacific Time, and ask to have a Commercial Relationship Manager in your area contact you.