CYBERSECURITY:
THE INDUSTRY'S NEXT FRONTIER

NEWPORT GROUP™

Findings from a 2018 DALBAR study of leading financial services firms on specific threats.

1. REDIRECT WITHDRAWAL

This may be the oldest trick in the book and predates the cyber era. The thief changes the address of record or direct deposit instructions on targeted accounts to that of the thief. This is followed by the thief terminating the account or making a permitted withdrawal so the proceeds are sent to the thief.

2. RECLASSIFY AN ASSET

More sophisticated thieves understand that some classes of assets are easier to liquidate than others, but changes among asset classes are less challenging. For example, liquidating an equity investment may introduce asset retention activities, but there may not be any encumbrances to an exchange. The sophisticated thief would open a money market fund with check writing privileges then exchange equity assets into the money market fund.

3. ROLLOVER SCAM

Recognizing the eagerness to capture rollover assets, the cyber thief can pinpoint targets of the right age to roll assets over into an account controlled by the thief. This would involve finding appropriate plan participants and a financial institution eager to capture the rollover. The thief gives the instruction to the financial institution, which then executes the rollover. The rollover account can then be emptied (net of withholdings).

4. POST MORTEM CLAIMS

This scheme takes advantage of the fact that the recording of deaths is notoriously slow. Searching death notices can give thieves a time advantage to empty financial accounts weeks and months before the scheme is discovered. When a new death notice is discovered for an individual, for whom the thief has data, accounts can be altered and funds withdrawn with little fear of discovery.

5. HARVESTING UNASSIGNED ACCOUNTS

Accounts with no advisor, broker or agent can be captured with an appropriate assignment to an impostor. Once assigned, the impostor can make changes, cancel policies and withdraw funds with impunity.

6. FIXING BAD EMAILS

A thief may send emails to stolen addresses and use the rejections to identify bad email addresses. The cunning thief simply contacts financial institutions asking to correct the bad email. Of course, the replacement email address is controlled by the thief. The email of record becomes a powerful tool for future activity by the thief.

CYBERSECURITY:
THE INDUSTRY'S NEXT FRONTIER

NEWPORT GROUP™

Findings from a 2018 DALBAR study of leading financial services firms on specific threats.

7. DISTRIBUTION OPTION CHANGE

Most investors elect to have dividends and capital gain distributions reinvested but cyber thieves may be able to change that option to a direct deposit cash payment. With a sufficiently large number of targets, such an activity could be highly profitable for thieves and devastating for financial services institutions.

8. AUTOMATIC WITHDRAWAL

Automatic withdrawals generally undergo less scrutiny than a partial or full withdrawal. Furthermore, after being set up there is seldom a review of the authenticity of the recipient. For thieves with enough information to overcome the automatic withdrawal hurdle, cash flow can continue undetected for years.

9. DEPOSIT AND WITHDRAW

Many institutions use a "next payment" form that includes the options to change an address. Using this form often bypasses the controls that exist for other address change tools. Replicating "next payment" forms with a small payment may be all that is necessary for a thief to attach his/her address to an account. This becomes the address of record and facilitates future payments to the thief.

10. RMD SHUFFLE

Thieves can take advantage of the fact that most retirement investors are unaware of the Required Minimum Distribution. This creates a window of opportunity before the deadline after reaching 70½ for thieves to manipulate the distribution for the first year.

Many of these methods begin with identifying accounts that exist. This is most easily done by login or a telephone call with key information (typically email address or phone number). If the attempt is rejected, it is assumed that an account does exist.

Newport Group has a number of protective measures in place to help prevent fraudulent activity, including two-factor authentication, business processes to notify participants of data changes or attempted account access, and frequent training programs that help our employees increase their awareness of email security.

To learn more, contact your Newport Group representative.