WINTER 2023 E-NEWSLETTER

At Digital Mountain, we assist our clients with their electronic discovery, digital forensics, cybersecurity, and data analytics needs. For this E-Newsletter, we discuss Business Email Compromise and financial loss in litigation settlements, relevant court cases, and best practices for prevention.

Preventing Fraudulent Fund Transfers

Fraudulent electronic fund transfers are big headaches for businesses and individuals alike. Thanks to sudden and dramatic increases in internet payments during the pandemic, fund transfer fraud also spiked rapidly. In late 2022, the FBI presented a report to Congress on Business Email Compromise stating that BEC-related losses for 2021 topped $2.4 billion, making it one of the fastest-growing categories of global cybercrime (https://www.fbi.gov/file-repository/fy-2022-fbi-congressional-report-business-email-compromise-and-real-estate-wire-fraud-111422.pdf/view). Unfortunately, there’s no way to stop all cybercrime, but we can and should take precautions to reduce opportunities for scammers to pick our proverbial pockets. Here are Digital Mountain’s suggestions:

Eliminate the Human Factor

Many fraudulent transfers begin with a social engineering phishing or whaling attack. With the proliferation of social networking accounts sharing occupations, titles, organization affiliations, and contact information, scammers can easily target employees by impersonating management and executive staff. That doesn’t mean you should shut down your social networking accounts; there are other sources through which a determined scam artist can find an organization’s information (website, press articles, industry associations, etc.). Beyond spam filtering software, we recommend the following six steps to reduce human error in email security:

1. Delete emails containing unknown links; use the preview pane to eliminate junk mail before opening.
2. Check email message headers for “close but not quite” user, account, and domain names that indicate account spoofing and takeover.

3. Don’t respond to out of the blue requests for information. Any instructions that are labeled “urgent,” “pay immediately,” or “I can’t take calls but need you to…,” should raise alarm bells.
4. Verify, preferably by phone, all details for fund transfers, especially if there’s a change to the usual process or account information.
5. Avoid sending data on accounts, customers, vendors, invoices, or other financial information to generic email accounts. If an email directs you to send a report to “accounting@” or “CFO@,” call and verify the request.
6. Have an IT person or a digital forensics expert such as Digital Mountain evaluate the Internet header information in the questionable email to determine its validity.

Keep Scammers Out of Your Email

Stopping scammers from accessing bank account information is often a matter of keeping phishing emails out of your email system. By ensuring that your email server has proactive security settings enabled, you can reduce the chances that a cybercriminal will sneak in.

Sender Policy Framework (SPF): SPF is a basic gatekeeper on the Outgoing Mail Server that also verifies that the domain from which the email is being sent is an approved domain. With SPF enabled, you can restrict emails being sent to only those from domains that your organization uses for email messaging.

Domain Keys Identified Mail (DKIM): DKIM relies on an encrypted signature, assigned by the sender’s email server, to verify that the owner of the domain authorized that mail transmission. With DKIM in place, a hash value is assigned automatically to the original message, basically locking in the content and header information. DKIM is hard to fool because the hash value signature is generated automatically, encrypted, and invisible to the end user.

Domain-based Mail Authentication Reporting and Conformance (DMARC): With SPF and DKIM in place, DMARC is the protocol that answers the question: Block, Quarantine, or Distribute? DMARC relies upon the results of SPF and DKIM to complete its mission, so if the message passes those tests, it's probably going to end up in the user’s inbox.

Banking (Cyber) Securely

Moving money is easier and faster thanks to internet-enabled banking functions. However, fast and easy doesn’t mean safe. Automated Clearing House (ACH) payments, which originate with the requester (payee), not the payor, are rich targets for cybercriminals. With the correct banking details frequently obtained by email scams, cybercriminals create payment demands that most banks will honor before alerting you to the request. ACH transfers operate on the assumption that you authorized the requesting party to remove regular or one-time payments. Business accounts may have only 24 or 48 hours to report a fraudulent ACH payment for any chance of reimbursement, and even then, there’s no hard and fast rule as to what the banking institution must do in response. Organizations and individuals can do more to protect their accounts from being accessed fraudulently:

1. Limit regular ACH payments to only those necessary. The less ACH payment activity, the easier spotting out of the ordinary activity may be. If you’ve been hit with a

fraudulent ACH withdrawal, you may need to suspend ACH debits entirely (if your bank allows it).

2. Guard your bank account details diligently. Printing banking instructions on paper for distribution is risky business, as is emailing the information without scrutiny.
3. Establish a relationship with your financial institution and let them know you are concerned about secure banking. Review their policies, procedures, and remedies before your account is accessed.
4. Review statements regularly. Even if you notice something odd after the reporting period, report it anyway.
5. Enroll in Positive Pay or Reverse Pay. With Positive Pay, an organization provides their financial institution with a list of checks that are “pre-approved” for payment. With Reverse Pay, the bank sends the account holder a list of all payments/checks presented against the account that day. The holder must approve or deny payments within the specified timeframe, or the payments will be made. Either way, the organization is responsible for communicating with the bank to prevent fraudulent payments from being processed, but the effort may pay for itself in thwarted fraud.
6. Set payment thresholds. Requiring secondary authorization on payments over a certain limit can lessen the opportunity for a large sum of money to disappear. However, many fraudulent withdrawals are actually a series of smaller amounts that are likely to go unnoticed.

When BEC leads to fraudulent electronic transfers, it represents a critical undermining of an organization’s comprehensive security goals. Once an organization’s email system and financial accounts are accessed by malicious actors, there’s every reason to call your financial institution to mitigate the financial losses. Here at Digital Mountain, we can help restore security measures, and assess and address remaining vulnerabilities. However, don’t delay taking some proactive steps to prevent BEC and banking fraud. A penny saved from a fraudulent wire transfer is still a penny earned.

Please direct questions and inquiries about electronic discovery, digital forensics, cybersecurity, and data analytics to info@digitalmountain.com.

UPCOMING INDUSTRY EVENTS

UF LAW's 10TH ANNUAL E-DISCOVERY CONFERENCE
Gainesville, FL: February 8-9, 2023

SOLID WEST 2023
San Francisco, CA: February 15, 2023

NETDILIGENCE CYBER RISK SUMMIT 2023
Ft. Lauderdale, FL: February 20-21, 2023

MASTER'S CONFERENCE FEBRUARY 2023
San Francisco, CA: February 22, 2023

ABA TECHSHOW 2023
Chicago, IL: March 1-4, 2023

Click here to see more upcoming events and links.

Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at various upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com.

DIGITAL MOUNTAIN, INC.
4633 Old Ironsides Drive, Suite 401
Santa Clara, CA 95054
866.DIG.DOCS

www.digitalmountain.com

Contact us today!

FOLLOW US AT: