PROTECTING AGAINST CYBER FRAUD

How to spot and prevent cyber fraud schemes

Nacha®

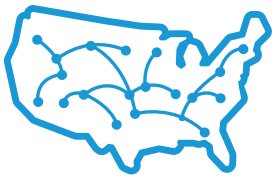
Updated October 2021

Table of Contents

Fraud schemes continue to grow, evolve and target legitimate businesses, nonprofits, government and other public sector organizations. The FBI monitors schemes like Business Email Compromise, Vendor Impersonation Fraud, and Mortgage Closing Scams, which typically involve social engineering or computer intrusion techniques.

2020 statistics show that 75,000 such schemes described in this booklet were reported and created losses of over $2.7 billion. The funds garnered from these schemes are directed to a fraudulent domestic account, usually using a money mule. Funds are quickly dispersed through cash or check withdrawals, gift cards, or conversion to cryptocurrency.[1]

These scams have been reported in all 50 states and in 177 countries with actual funds transfers occurring in at least 140 countries.[2]



Victim complaints filed with the IC3 and financial sources indicate the top states by number of victims are California, Florida, Texas, New York, and Illinois.[3]

In 2020 IC3 received 792,000 complaints covering all cyber-related crimes, citing losses of $4.1B.[4]

Business Email Compromise – What Is It?

With Business Email Compromise, legitimate business email accounts are either compromised or impersonated, and then used to order or request the transfer of funds. The fraudster will often compromise one of the business' officers and monitor his or her account for patterns, contacts and information. Using information gained from social media or "out of office" messages, the fraudster will often wait until the officer is away on business to use the compromised email account to send payment instructions.

How It's Done

Fraudster monitors officer's accounts for patterns, contacts and information.

After identifying the target, ploys are conducted such as spear-phishing, social engineering, identity theft, email spoofing, and the use of malware to either gain access to or convincingly impersonate the email account.

Fraudster uses the compromised or impersonated account to send payment instructions.

Payment instructions direct the funds to an account controlled by the fraudster or a money mule.

1-4. https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

Business Email Compromise – Avoid Being a Victim

Solid internal controls are key to guarding against these scams.

- Understand these attacks can come via email, phone calls, faxes or letters in the mail. Don't assume it's a cybersecurity problem.
- Educate and train employees to recognize, question, and independently authenticate changes in payment instructions, payment methods (e.g., ACH to wire), or pressure to act quickly or secretively.
- Be old-fashioned! Verbally authenticate any changes via the telephone.
- Review accounts frequently.
- Initiate payments using dual controls.
- Never provide password, username, authentication credentials, or account information when contacted.
- Don't provide nonpublic business information on social media.
- Avoid free web-based email accounts for business purposes. A company domain should always be used in business emails.
- To make impersonation harder, consider registering domains that closely resemble the company's actual domain.
- Do not use the "reply" option when authenticating emails for payment requests. Instead, use the "forward" option and type in the correct email address or select from a known address book.

5. https://www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise

> "The best way to avoid being exploited is to verify the authenticity of requests to send money by walking into the CEO's office or speaking to him or her directly on the phone. Don't rely on email alone."

– FBI Special Agent Martin Licciard[5]

Vendor Impersonation Fraud – What Is It?

Vendor Impersonation Fraud can occur when a business, public sector agency or organization, e.g., a municipal government agency, a school district, receives an unsolicited request, purportedly from a valid contractor, to update the payment information for that contractor. The update could be new routing and account information for ACH or wire payments, or a request to change the payment method from check to ACH or wire payment along with routing and account information. This type of request could come from fraudsters and not the contractor or construction-related company. Although any business entity could be the target of this type of social engineering attack, public sector entities seem to be specifically targeted because their contracting information is oftentimes a matter of public record.

How It's Done

Fraudster monitors a business, public sector agency or organization for publicly available contractor or vendor information.

The fraudster poses as a legitimate vendor or contractor to request updates or changes to payment information, or change of payment method.

Then the fraudster, sends an email, form, or letter resulting in the business or agency transferring funds to an account controlled by the fraudster or a money mule.

Vendor Impersonation – Avoid Being a Victim

Solid internal controls are key to guarding against these scams.

- Understand these attacks can come via email, phone calls, faxes or letters in the mail. Don't assume this is a cybersecurity issue.
- Educate and train employees to recognize, question, and independently authenticate changes in payment instructions, requests for secrecy, pressure to take action quickly, and any change of payment method (e.g., ACH to wire).
- Be old-fashioned! Verbally authenticate any payment changes via the telephone.
- Review accounts frequently.
- Initiate payments using dual controls.
- Do not provide nonpublic business information on social media.
- Do not use the "reply" option when authenticating emails for payment requests. Instead, use the "forward" option and type in the correct email address or select from a known address book.
- Make vendor payment forms available only via secure means or to known entities.
- Require changes to payment account information be made or confirmed only by site administrators, and use methods like verification codes to existing contacts.
- Do not ignore calls from a financial institution questioning the legitimacy of a payment.

Payroll Impersonation Fraud – What Is It?

Fraudsters target individual employees by directing the employees to update or confirm their payroll information via a fake payroll platform that spoofs their employer's actual payroll platform. In some cases, the fraudster may claim the employee must do one of these: view a confidential email from human resources or the payroll department, view changes to the employee's account, or confirm that the account should not be deleted. In any case, when the employee logs in from a link or attachment in the email, the fraudsters then use the stolen employee credentials to change payment information in the real payroll platform.

How It's Done

Fraudster targets an employee by sending a phishing email that impersonates the employee's human resources or payroll department, as well as the company's payroll platform. The email directs the employee to log in to confirm or update payroll information, including bank account information.

Employee clicks the link or opens the attachment within the email and confirms or updates the payroll information.

The fraudster then uses the stolen login credentials to change payment information to an account controlled by the fraudster or a money mule.

Payroll Impersonation – Avoid Being a Victim

- Employers should alert employees to watch for phishing attacks and suspicious malware links.
- Employees should be directed to check the actual sender email address, rather than just looking at the subject line, to verify that the email came from their employer or payroll service provider.
- Employees should not reply to any suspicious email; instead have them forward the email to a company security contact.
- Employees should not enter their login credentials when clicking on a link or opening an attachment in an email.
- Employer self-service platforms should authenticate requests to change payment information using previously known contact information. For example, requiring users to enter a second password that is emailed to an existing email address, or to use a hard token code.
- Employer self-service platforms also should reauthenticate users accessing the system from unrecognized devices, using previously known contact information.
- Set up alerts on self-service platforms for administrators so that unusual activity may be caught before money is lost. Alerts may include when banking information is changed, and multiple changes that use the same new routing number or identical account numbers.
- Employers should consider validating employees' new Direct Deposit information by sending ACH prenotification transactions.

Mortgage Closing Scams – What Is It?

In many real estate transactions, it is common for homebuyers, real estate agents, law firms, and title and settlement companies to exchange information about the transaction and settlement via email. Mortgage Closing Scams are when a fraudster gains knowledge of a real estate settlement, and impersonates one of the parties to the settlement in order to redirect funds transfers at, or near, the time of the transaction settlement. In many cases, emails purportedly from the real estate agent, real estate lawyer or settlement agent are sent to the homebuyer containing "new" payment instructions, and could even demand the down payment be sent just before the closing date. In other cases, the fraudsters pose as the seller and send changes to payment instructions to the real estate lawyer or settlement agent in order to redirect the proceeds of the sale to an account under their control, probably using a money mule. Some cases also involve phone calls from the fraudsters to "verify" personal information regarding the real estate transaction.

Because participants in real estate settlements commonly use irrevocable wire transfers, funds sent to fraudsters' accounts are redirected or withdrawn quickly and are unrecoverable.

Recent FBI statistics show that approximately 1,137 such schemes are reported each month and create victim losses of over $17 million per month.[6] The FBI says, "Victims most often report a spoofed e-mail being sent or received on behalf of one of these real estate transaction participants with instructions directing the recipient to change the payment type and/or payment location to a fraudulent account. The funds are usually directed to a fraudulent domestic account which quickly disperse through cash or check withdrawals."

How It's Done

Fraudster employs use of malware to gain access to email accounts.

Email traffic is monitored regarding the real estate transaction, closely following closing/settlement dates and payment instructions.

After identifying the target, the fraudster impersonates a party to a real estate settlement transaction.

The fraudster provides new account information and instructions for a pre-settlement payment, usually by wire transfer.

Payment instructions direct the funds to an account controlled by the fraudster, or a money mule.

6. https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

Mortgage Closing Scams – Avoid Being a Victim

Financial Institutions:

- Make real estate industry customers such as real estate brokerages and title and settlement companies aware of this fraud.
  - Consider establishing code phrases known only to the parties. For example, a phrase that is meaningful to the parties, but uncommon to others.
- Through your mortgage division, educate homebuyers of this scheme.
  - Establish procedures that require verification of payment type and bank account information before funds disbursement.

Consumers:

- As with all types of email phishing or spoofing schemes, consumers should be skeptical of emails containing changes to payment instructions.
- Verify all emails and phone calls, especially if revised or new payment instructions, or a change of communication method are provided. Use known phone numbers to call and verify the contents of the email or voice request.
- Avoid clicking links in emails. Check first with a trusted representative such as your real estate agent or settlement agent, to verify that they sent the email. Do not send sensitive information via email.

Confidence Scams/Romance Scams – What Is It?

With Confidence/Romance Scams, the fraudster deceives the victim into believing they have a trusted relationship, be it friend, family, or romantic, and leverages that relationship to persuade the victim to send money, provide personal financial information, or purchase gift cards. Fraudsters often say they are working outside the United States or being held from returning to the United States, thereby avoiding meeting in person.

How It's Done

Fraudster creates fake profiles on sites or apps, and contacts the victim through social media.

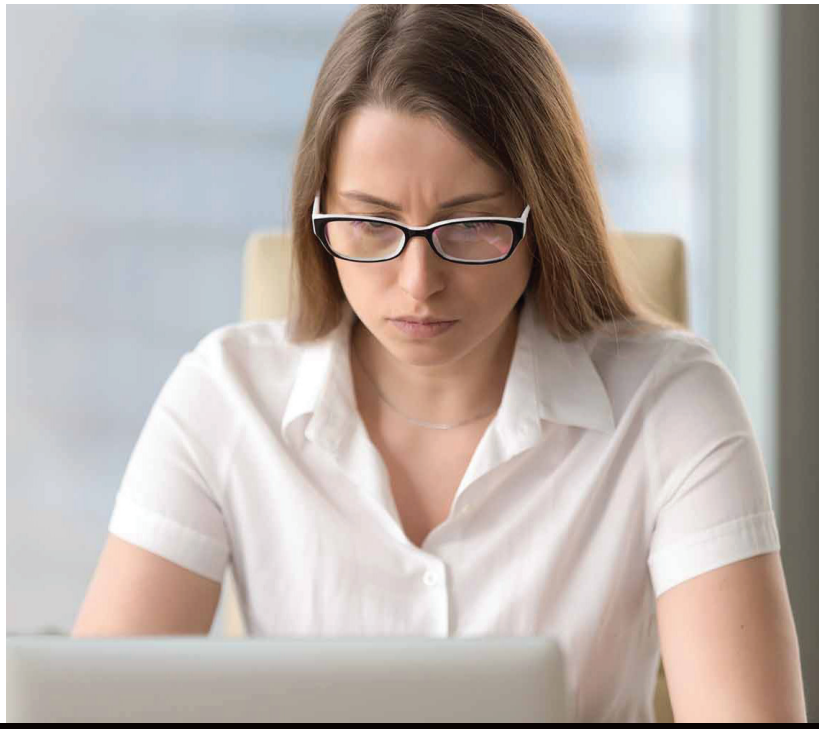
Fraudster builds trust and gains their confidence by using the illusion of a romantic or close relationship.

Fraudster will eventually ask for money using reasons such as a medical emergency or unexpected legal fees.

Payment instructions direct the funds to an account controlled by the fraudster, or a money mule.

Confidence Scams/Romance Scams – Avoid Being a Victim

- Be careful what is posted on social media and other public sites. The fraudster will use this information to target you.
- Research the person's photo and profile using online searches.
- Beware if the person asks you to leave the platform where you "met" and communicate directly by text or phone.
- Proceed with caution if the person attempts to isolate you from friends and family.
- Beware if the person promises to meet in person, but then always comes up with a reason to postpone.
- Never send money to anyone you have only communicated with online or by phone.



Ransomware Attacks – What Is It?

Ransomware is a type of malware that will prevent you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data.

How It's Done

The fraudster successfully installs ransomware onto a computer by sending an email attachment, ad, link, or website that's embedded with malware.

Once the code is loaded on a computer, it will lock access to the computer itself or data and files stored there. More nefarious versions can encrypt files and folders on local drives, attached drives, and even networked computers.

You usually discover it when you can no longer access your data or you see computer messages letting you know about the attack and demanding ransom payments.

Ransomware Attacks – Avoid Being a Victim

- Be cautious and conscientious when it comes to clicking on links or downloading.
- Keep operating systems, software, and applications current and up to date.
- Make sure anti-virus and anti-malware solutions automatically update and regularly run scans.
- Back up data regularly and ensure backups were complete.
- Secure the backups. Backups should not be connected to the computers/network they are backing up.
- Create a continuity plan in case your organization is the victim of an attack.

Key Terms

Malware: Malicious software including viruses, ransomware, and spyware, typically consisting of code designed to cause extensive damage to data and systems or to gain unauthorized access.

Money Mule: Someone who transfers or moves illegally acquired money on behalf of a fraudster. Fraudsters recruit money mules to help launder proceeds derived from the schemes described in this booklet.

Social Engineering: The use of deception to manipulate individuals into providing confidential or personal information.

Spear-phishing: Sending emails supposedly from a known or trusted sender in order to induce the recipient to reveal confidential information.

Spoofing: Disguising an email from an unknown source as being from a known, trusted source.

Nacha®