STEPS ORGANIZATIONS CAN TAKE TO PREVENT SCAMS AND PROTECT THEMSELVES

From startups to large corporations, organizations of every size may have to manage the potential financial losses and operational disruptions caused by scams. Organizations are attractive targets because of their higher account balances that could result in larger scam payments, compared to smaller consumer accounts. In addition, it can be easier for criminals to insert themselves into existing business processes to steal money rather than building a relationship with individuals over time. Protecting organizational brands involves processes and controls, employee training and secure technology for communications and information.

PROCESSES AND CONTROLS

Criminals use scams as a path to access money and information.

For any process that involves moving money or generating a payment, adding appropriate controls can help reduce the chance for a payment to be sent due to a scam. Examples of controls that could mitigate scams include:

- **User entitlements:** Control access to internal payment systems and online banking based on an employee's role
- **Dual approval:** Payment requests and approvals performed by two or more employees
- **Employee payment limits:** Establish dollar limits for payment requests, approvals and maximum daily payment totals based on employee roles
- **Validate changes to payment instructions:** Confirm changes to existing payment details for vendors through a separate contact or source
- **Payee confirmation for new receivers:** Confirm the payee account details when a new payee is added
- **Reconciliation:** Compare payments on account statements to accounts payable details to identify anomalies
- **Review employee audit logs:** Identify unusual user access or activity
- **Account alerts:** Set up payment notifications through the financial institution based on parameters, such as dollar amount, payment type or payee
- **Invoice validation:** Review invoices submitted for payment to confirm the products or services were delivered

STEPS ORGANIZATIONS CAN TAKE TO PREVENT SCAMS AND PROTECT THEMSELVES

EMPLOYEE TRAINING AND AWARENESS

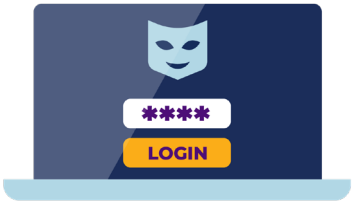
Criminals pose as representatives of legitimate entities — such as financial institutions, vendors or customers — to manipulate employees into sending payments or providing sensitive information. For example, business email compromise scams, where a criminal poses as a vendor to request a change to payment instructions, are a continuing threat to organizations. Employees who are aware of these and other scams and tactics are better equipped to identify and prevent them. Organizations can actively engage their employees to help prevent scams by:

- Training them to identify relevant scam trends and tactics
- Conducting regular testing of employees to spot phishing emails and scam attempts — and reinforce the need for vigilance
- Creating an environment where employees are encouraged to escalate unusual or suspicious requests
- Helping employees understand their role and shared accountability to prevent scams, as well as the importance of processes and controls

Scam Prevention Use Case: Employee Training and Awareness

Criminals impersonate legitimate mortgage lenders and title companies to redirect money for real estate transactions. This typically occurs when criminals gain access to email exchanges for buying or refinancing a property. Criminals send an email that appears to be from the lender or title company with payment instructions to redirect the down payment and closing costs to an account they control. Mortgage and title companies recognize the risk to buyers from this scam. In response, companies often proactively notify their customers to be alert for the potential risk of spoofed emails and independently verify any change to payment instructions. They describe the closing process steps and specify the legitimate payment instructions so customers know what should happen. Mortgage and title companies often provide training to their employees to be aware of these scams and work with customers to prevent scam payments.

SECURE DEVICES, SYSTEMS AND INFORMATION



A critical part of scam prevention is stopping fraudulent requests before they cause harm. A strong cybersecurity framework can help protect technology and systems from unauthorized access. For example, antivirus and anti-malware software can detect and quarantine phishing and spam emails and prevent or restrict downloading potentially harmful files from the internet. Policies and procedures can support this framework by requiring employees to use strong passwords, multi-factor authentication, virtual private networks (VPNs) and secure Wi-Fi networks for access to systems and data. Organizations with strong protocols for use and disclosure of information can reduce the chance of employees falling for social engineering tactics when asked to release company or customer-specific information. Encrypting information when stored or transmitted is another way to deter criminals.

STEPS ORGANIZATIONS CAN TAKE TO PREVENT SCAMS AND PROTECT THEMSELVES

PROTECTING ORGANIZATION BRANDS

To add to their credibility, criminals often make scam requests that appear to be sent by legitimate organizations. Organizations can take steps to protect their digital platforms and communications to help protect their brands from the negative impact of impersonation.

- Prevent and take down fake websites and applications by:
  - Identifying sites that may be used for phishing information, selling non-existent merchandise or spreading malware
  - Monitoring domain registrations to detect internet websites with close internet address variations from legitimate company websites
  - Registering similar variations of website addresses or domain extensions to avoid their use by criminals, if these website addresses are available
- Authenticate emails to prevent phishing emails and spam by:
  - Using email authentication protocols to identify unauthorized use of registered business email domains
  - Providing an option for customers to report phishing emails
- Protect phone numbers and text messages by:
  - Using a trusted telecom provider with services to authenticate phone calls and text messages, as well as identify spoofing of registered phone numbers
  - Enabling phone number authentication protocols — digital signatures to verify the origin of the call — to counter caller ID spoofing used for impersonation scams

TAKE STEPS TO PROTECT YOUR ORGANIZATION

In the fight against scams, organizations play a crucial role in protecting their operations, customers, vendors and brand. Establishing controls, emphasizing employee training and implementing technology can make it harder for criminals to commit scams — which in turn, benefits all organizations.

The scams mitigation toolkit was developed by the Federal Reserve to help educate the industry about scams and outline potential ways to help detect and mitigate this fraud type. Insights for this toolkit were provided through interviews with industry experts, publicly available research, and team member expertise. This toolkit is not intended to result in any regulatory or reporting requirements, imply any liabilities for fraud loss, or confer any legal status, legal definitions, or legal rights or responsibilities. While use of this toolkit throughout the industry is encouraged, utilization of the toolkit is voluntary at the discretion of each individual entity. Absent written consent, this toolkit may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.