Risk Mitigation for Phishing Attacks

Elavon continues to educate and inform our Customers of current fraud trends. Please review the following information referencing the various forms of malware and phishing scams used by criminals.

Obtaining Access Through Phishing

Criminals are currently using traditional phishing techniques to obtain the Customer’s account credentials. For example, a criminal calls or sends an email message to a customer purporting to be a member of a Payment Network (Visa, MasterCard, Discover, American Express, etc.), the customer’s processor, service provider, or acquiring bank and indicates that the customer’s account has been suspended. The criminal requests sensitive customer account credentials, such as the customer’s user ID, password, customer identification (MID) number, and terminal identification number in order to lift the suspension. Once the customer provides the information, the criminal replies that the customer’s account has been reinstated.

Performing Test Transactions Through Brute Force

Once the criminal hacker has gained network access, the customer’s terminal or system can be exploited as a venue for performing test transactions. The hacker’s own high-speed computer programs submit numerous authorization requests for small dollar amounts using stolen card account information from victims of other phishing scams in combination with sequential three-digit card validation code 1 (CVC 1) values (such as 999, 998, 997, and so on) until the hacker receives a valid authorization (that is, the CVC 1 value matches the stolen account number). When accessing an online customer’s system, the system is manipulated to mimic a swiped transaction at a retail terminal. These submitted authorization requests can accumulate into the thousands in just a short period of time.

Defending Against Phishing Attempts

Customers should perform the following risk mitigation measures:

- Use caution when providing sensitive information, such as user IDs and passwords.
- Do not provide sensitive information to anyone, unless certain of the credentials of the potential recipient of the information.
  - Guard terminal information.
  - Do not give out the MID number or the terminal identification number (TID).
  - Payment Networks acquirers, and processors already have this information and would not request it.
  - Therefore, if a call is received requesting this information, it is likely a phishing attempt by a criminal to gain terminal access. Instead, call your acquirer or processor, ask to be transferred to the appropriate person or department that handles your customer account, and report the call that you received.
- Avoid clicking on hyperlinks within email communications. Type the URL into the web browser instead.
- Do not download suspicious attachments.
- Instruct employees not to use business computers and workstations for non-business activities, such as web browsing or checking personal email.
• When reviewing or responding to email messages, ensure that the sender’s information is correct. Be vigilant for slight misspellings, which may indicate a phishing attempt.

• If the customer receives a phone call, email message, or repair technician visit that is suspicious, the customer should not respond or provide any information. Immediately contact the processor or acquirer to verify the legitimacy of the request.

• Beware of any unscheduled terminal repair technician arriving at a customer’s location requesting access to the point-of-sale (POS) terminal. The technician may be a criminal attempting to gain access. If a repair technician arrives unannounced, contact the acquirer or processor to verify the technician’s identity using contact information on file, not the contact information provided by the technician.

• Educate staff regarding anti-phishing strategies, such as only opening email messages from a known or trusted source.

• Limit employee access to the MID number, terminal identification number, or an acquirer’s BIN to help prevent unintentional leaking of this information to a criminal.