Financial Fraud: *Digital Skimming*

Digital skimming is when a threat actor deploys malicious code onto a merchant's website, typically targeting the checkout pages, in order to harvest payment account data. The data collected from digital skimming can include primary account number (PAN), card verification value (CVV), card expiration date, and other personal identifiable information (PII).

Threat actors are able to conduct digital skimming by exploiting gaps in security controls on a merchant's website.

Phishing websites mirror real websites to trick you into revealing your payment account and personal details.

A few signs to watch out for: the wrong URL, spelling errors, designs or website pages that don't look right.

Fraud Prevention Recommendations

- **Use cybersecurity best practices**, including enabling anti-phishing protection on your web browser, adding multi-factor authentication to account log ins, using unique, strong passwords for different accounts, not clicking on unsolicited links, and remain vigilant of the URLs you are visiting.

- **Look for the "s" –** When paying online, check the URL to ensure it begins with "http**s**://". The "s" at the end indicates a secure connection.
Additionally, check that the name of the web page does not contain spelling errors or strange characters.

- **Update system and application software** – Install the latest software on your computer, tablet, or phone from legitimate and verified sources.

- **Use tokens when possible.** A token can be viewed as a "secret code" that contains no customer or sensitive data, which can be used to transmit a payment. Use of a token for a purchase, or tokenization, is the digital equivalent of using a card's chip for in-person purchase. The value of the token changes with each transaction, making them more resistant to use by fraudsters.

- **Review bills, bank statements, and credit reports** to identify unauthorized charges, and **sign up for purchase alerts** with your card issuer to notify you in certain situations, such as when your account reaches a spending threshold, makes an international transaction, makes an online transaction, or if suspicious activity is suspected on your account.

To learn more about protecting yourself from financial fraud, visit:
https://usa.visa.com/visa-everywhere/blog.html

VISA
everywhere you want to be