



TECH LINK

Protect Your Heart (and Your Data) from Valentine's Day Scams

Valentine's Day is a time for love and affection, but all of those emotions can leave you vulnerable to cyber threats. Take off the rose-colored glasses to protect your heart and your data this Valentine's Day with these tips:

- **Beware of "Too Good to Be True" Gift Offers and Deals:** Scammers often use fake discounts or flash sales for luxury gifts, meals and hotels around Valentine's Day to lure victims. Always verify the sender's email (or web) address and avoid clicking on suspicious links.
- **Verify Digital E-Card Senders:** Cybercriminals exploit digital e-cards to send malware or phishing links. If you receive a digital Valentine's from an unexpected sender, verify it with the supposed sender via text or call directly.
- **Spot "Phishing Cupid" Emails:** Scammers may impersonate delivery services or colleagues sending a "secret Valentine." You could also be sent an irresistible email offer for a Valentine's gift, or an e-card purportedly from an admirer you may or may not know, that turns out to be a phishing attack. These emails often ask you to log in or provide personal details. Educate others and use secure payment methods when buying gifts online.
- **Say No to Romance Scams:** Sometimes a bad actor will take advantage of loneliness and our human nature to connect with others by manipulating victims into sending money or disclosing personal information. These threats have become even harder to spot in the wake of AI. Not everything is as it seems—do your own research thoroughly before engaging any of these inquiries.
- **Use Secure Payments:** Stick to well-known retailers and secure payment methods (e.g., PayPal, credit cards) with reputable dispute processes.



By applying these tips, you can celebrate Valentine's Day safely and protect your personal information (and your wallet) from cyber threats.

New Year = More Scams

It may be a New Year, but scammers are up to the same old tricks. MVEC has recently become aware of scams where a fraudster poses as an MVEC representative or that of our power supplier, insisting on immediate payment to prevent disconnection. Neither MVEC nor our power supplier will call to demand instant payment. We want to keep you safe: If you're ever unsure about the person on the other end of the line, please hang up and reach out to us directly. We're always here to help you verify your account safely.

If you receive a suspicious call, text, or email:

- **Hang up immediately.**
- **Do not call any phone numbers provided by the solicitor.**
- **Contact MVEC directly at 800-927-6068 or 319-462-3542 to verify your account status.**