U.S. Small Business Administration

Cybersecurity Tips:

Social Media and Scams

Social media provides users the ability to exchange thoughts and ideas with people from corners of the worlds they might not have visited, enables strangers to collaborate and positively impact our collective society, and increase awareness to help grow our businesses and communities. However, social media is a double-edged sword, for all the good we intend to accomplish, social media is also an adversary breeding ground for subverting social media use for their illicit gain.

Misinformation

Quick dissemination and viral posts allow adversaries to spread misinformation and "fake news" through deepfake accounts, bots, big data, and trolls. To identify misinformation:

- Scrutinize and exercise skepticism when reading about divisive and emotionally charged topics
- Verify the information or claims online through reliable sources
- Search for additional social media accounts for the person to verify their identity
- inspect the content posted

Phishing & Scams

Phishing scams are one of the most common forms of social engineering tactics used by adversaries to fraudulently acquire a recipient's personally identifiable information (PII). Examples of PII include credit card and bank account numbers, debit card PINs, and account credentials. To identify phishing on social media look out for:

- Poor spelling and grammar
- Threats requiring a sense of urgency
- Spoofed or purported websites, domains, or company logo and imagery

Malware

Links available from untrusted or unsolicited social media accounts, profiles, and messages can be boobytrapped to deliver malware to your devices. To reduce the risk of malware:

- Use and update Anti-Virus/Endpoint protection software
- Install reputable security applications on your mobile devices
- Always keep browser and applications updated
- Be wary of applications and links from untrusted or unsolicited sources

Account Takeovers

Account Takeovers can result in the loss of control of social media accounts. The key to taking over these accounts is commonly through your most popular form of online identity, your email address. To protect against account takeovers:

- Use Multi-Factor Authentication (MFA) for social media and email access
- Use strong, complex passwords
- Don't reuse passwords
- Don't use unsolicited links to access social media. Type in the URL directly into the address bar
- Consider using separate emails for sensitive websites, platforms, and accounts