PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

Cyber Protection Through Awareness

Be Alert to Five Cyber Scams

By Thomas DeMayo, Partner and Robert Gaines, Director

As the cyberthreat landscape continues to evolve, not only must our technical defenses become more sophisticated, our awareness is also equally essential. We have all encountered scams in many different forms, either professionally or personally, and countless individuals and companies have experienced losses from cybercrime.

As the holidays approach — and Cybersecurity Awareness Month comes to a close — following is a list of the five most common cyberscams today, along with both preventative measures and steps to take if you fall victim. While these are the basics, in many respects, they are the most powerful.

1. Phishing (Email and SMS)

Phishing is probably the most common threat we all experience. Attackers send emails or text messages designed to lure us into taking action by making an emotional connection with us. It is that emotional connection that we need to control, resisting the knee jerk reaction to respond, taking a deep breath and pausing, inspecting and thinking before acting.

Prevention:

- Don't respond to unsolicited emails or texts asking for personal or financial information.
- Double-check the sender's email address (i.e., the sender says "Amazon Prime," but the address is info@lv02.benchia111.shop). Remember, the email address is inside the brackets (e.g. <tdemayo@pkfod.com>). That is the component of the address you must absolutely ensure is spelled correctly.
- Verify the authenticity of the request, if necessary, by logging into your account or calling the support number noted on the website.
- Avoid clicking links or downloading attachments from sources you don't know or trust.
- Use multi-factor authentication (MFA) to secure your accounts.

If victimized:

- Immediately change the passwords of your compromised accounts.
- On the account you feel may have been victimized, utilize the option to sign out of all existing sessions.
- Monitor your financial accounts for unauthorized transactions.

2. Impersonation Scams (CEO Fraud, Fake Customer Support)

Attackers impersonate a high-level executive in your business, vendors you may interact with or customer service agents from a business you know to trick you into transferring money or sharing personal information. These messages often have a sense of urgency so that you feel the need to act quickly before verifying the sender.

Prevention:

- Verify the identity of anyone requesting sensitive information or transfers, especially if the request seems urgent or unusual. It is best to do this through known communication channels (email or phone) – don't reply to the original message.
- Scammers can fake caller ID; if you are unsure of the contact's identity or source, call the organization directly using a verified phone number.
- Be cautious when receiving customer support calls from technology companies or banks, as they rarely initiate communications via phone or text messages.
- Always be suspicious of requests for gift cards and never provide the account details.

If victimized:

- Notify the affected company or individual immediately.
- Alert your bank or financial institution to stop any unauthorized transactions.

3. Online Shopping Scams

Scammers create fake websites or online stores offering you counterfeit or non-existent products. Once you provide your purchase details, they never send the product and frequently make additional charges using the information you provided. Fake websites are very sophisticated and look legitimate to most users.

Prevention:

- Shop only on reputable websites.
- Look for grammar and spelling errors that may indicate that the site is fake.
- Avoid shopping on sites that you have been redirected to via social media or advertising, as they may be counterfeit.
- Read reviews and do background checks on unfamiliar websites. Compare the details with your chosen shopping sites (i.e., Amazon, Shopify, eBay, etc.).
- Use a credit card for online purchases, as it offers better fraud protection.

If victimized:

- Contact your bank or credit card company to dispute the charges.
- Report the fake site to the FTC (ReportFraud.ftc.gov).
- If the site is international, report it to Econsumer (https://www.econsumer.gov/).
- Change your passwords if any account information was shared.

4. Fake App Scams

Scammers create fake mobile apps that look like real ones to steal account credentials and your personal data or they install malicious software that is hard for you to detect. Fake apps are difficult to detect and often look identical to the real ones they are impersonating. In most cases, it is not until money has been lost or the information already stolen by the time the user realizes what has occurred.

Prevention:

- Only download apps from official app stores (e.g., Google Play, Apple Store) on your device.
- Check the app icon to make sure it matches what is displayed or referenced on the company's website. Fake apps often have low-quality branding and icons.
- Check app reviews, download count, release date, developer information and permissions before downloading.

- Use mobile security software to detect malicious apps (e.g., Norton, Bitdefender, McAfee).

If victimized:

- Delete the fake app immediately and run a security scan on your device.
- Change the login details for any accounts that may have been compromised.
- Report the fake app to the app store.

5. Credential Stuffing

Attackers use stolen usernames and passwords taken from previous data breaches (e.g., Yahoo, LinkedIn, Equifax, etc.) to try to access other accounts where the same credentials might be used. These are effective attacks because users often use the same username and password on multiple websites.

Prevention:

- Use a password manager (e.g., LastPass, Keeper or 1Password) to store and generate passwords securely.
- Use unique, strong passwords for each account; never reuse passwords.
- Enable MFA wherever possible.
- Avoid storing passwords and personal information in your browser, as it can be recovered if your device is stolen.

If victimized:

- Change the passwords for all impacted accounts.
- Monitor your accounts for unusual activity.
- Report the incident to affected service providers and ask them to help secure your account.

Protecting Your Identity

If you have fallen victim to any of these scams and it resulted in a compromise of sensitive personal information such as your Social Security number, there are some additional steps you can take to protect your identity. Our advice is to assume your identity is already stolen and take the measures below as a precautionary action:

- Contact the three major credit bureaus (i.e., Equifax, Experian, and TransUnion) to freeze your credit and to prevent new accounts from being opened in your name. Keep in mind, once you do this, you will need to "thaw" your credit record with all three bureaus when you want to open a new credit line.
- Consider using a credit monitoring service to keep track of any changes to your credit report. The service should alert you to any key changes or inquiries.
- Lock your Social Security number in E-Verify to protect it from being used by someone else to gain employment fraudulently.
- Get an identity protection (IP) PIN from the IRS to prevent someone else from filing a tax return using your Social Security number.
- If you know someone over 60 who has been scammed, you can contact the National Elder Fraud Hotline at 1-833-FRAUD–11 (833-372-8311).

Contact Us

We have a dedicated team of cybersecurity and privacy professionals available to assist your company navigate the cyber landscape, mature and test your cybersecurity program and/or educate your staff on how to avoid becoming a victim. Please contact your client service team if you need assistance or:

Thomas J. DeMayo, CISSP, CISA, CIPP/US, CRISC, CEH, CHFI, CCFE
Partner
Cybersecurity and Privacy Advisory
tdemayo@pkfod.com | 646.449.6353

Robert Gaines, CISSP, CECI, CCFI, CIPP/US
Director
Cybersecurity and Privacy Advisory
rgaines@pkfod.com | 425.518.1974