ACCP
Association of Corporate Citizenship Professionals

ACCP's Practices for Safeguarding Against Phishing and Identity Theft

Purpose: To protect our organization, vendors, and members from phishing and identity theft attempts.

Scope: This applies to all members, contacts and third-party vendors.

Statement: We are dedicated to minimizing cyber risks associated with phishing - ensuring that everyone can conduct business with ACCP safely. To support this goal, we are sharing our standard practices and essential security awareness information with stakeholders and ask that readers familiarize themselves with our policies.

Our Standard Practices:

1. **Bank Routing Number Changes**
   a. **Our Practice:** We will never email members and vendors asking them to change the bank routing number without calling first.
   b. **Reason:** Cybercriminals may attempt to change payment details via email to divert funds into their accounts.
   c. **Action:** If you receive an email from ACCP asking to change the routing number, report it to your company's Cybersecurity department and alert ACCP of the activity by e-mailing accounts@accp.org.
2. **Payment Methods**
   a. **Our Practice:** We accept ACH and credit card payments. We do not accept payment via bitcoin. We only accept wire transfers in rare situations when ACH is not an option. Credit card payments are only processed through our website at www.accp.org.
   b. **Reason:** These payment methods are frequently exploited by cybercriminals for fraudulent transactions.
   c. **Action:** Please contact accounts@accp.org if you'd like more information about paying via ACH or any other method.
3. **We Will Never Ask for Gift Card Payments**
   a. **Our Practice:** We will never ask members and vendors to pay in gift cards of any type – including iTunes, Amazon, eBay, Visa, and other prepaid cards.
   b. **Reason:** Cybercriminals often send unsolicited emails or calls asking people to buy gift cards. Be especially careful during high-profile or newsworthy events – like elections - when scammers increase their phishing attempts.

4. **Unnecessary Pressure**
   1. **Our Practice:** We will never pressure members or vendors into taking immediate action via email or text because a staff person, board member or the organization is in trouble etc. [*Note: In the final days prior to an educational event hosted by ACCP, we may send a link to register on our website. Please review the content of the ask to be sure that the action aligns with the date sensitive opportunity.*]
   2. **Reason:** Cybercriminals use pressure to trick you into acting impulsively, such as asking you for help because an organization or person is in a troubled situation.
5. **Requests for Sensitive Information**
   1. **Our Practice:** We will never ask for sensitive information via email or text, such as Social Security numbers, passwords, or payment details.
   2. **Reason:** Cybercriminals often create fake websites that look like legitimate organizations. If a link in a phishing email is clicked and information entered, these criminals can access sensitive information.
6. **Shipping or Purchase Emails**
   1. **Our Practice:** We will never send members or vendors an ***unexpected email*** about shipping delays or purchase confirmations.
   2. **Reason:** During peak shopping times, cybercriminals send a lot of fake shipping or purchase emails to steal login credentials, install malware, or obtain financial details.
7. **Email Attachments**
   1. **Our Practice:** We will never send ***unsolicited email attachments***.
   2. **Reason:** Cybercriminals often send attachments containing malware. If you receive an unexpected attachment, do not open the attachment.
8. **QR Codes**
   1. **Our Practice:** We will never send a QR code in an email.
   2. **Reason:** Cybercriminals use QR codes to phish their victims. Unlike links, where you can hover to check where you're being directed, these codes make it impossible to know if they're legitimate. Watch out for emails sent outside of business hours and those that contain spelling or grammatical errors.

Additional Security Awareness Tips:

- **Always Verify Requests**: Double-check the sender's email address and look for any signs of impersonation or inconsistency. Confirm unexpected requests through a different communication channel, such as a phone call.
- **Be Wary of Links and Attachments**: Don't click links or open attachments from unknown or unexpected sources.

- **Guard Sensitive Information**: Do not share sensitive personal information via email or text.
- **Use Strong, Unique Passwords**: Create strong passwords for each account and change them regularly.
- **Enable Multi-Factor Authentication (MFA)**: Add an extra layer of security by enabling MFA wherever possible.
- **Report Suspicious Activity**: Report suspicious emails, texts, or calls to your IT department immediately. When you know they are not legitimate, block the account.

If you are worried about your vulnerability to phishing or fraud campaigns, contact our security partner, Teal. They can help you develop a comprehensive plan to mitigate risks to your business, just as they do for us.

Together, we can protect the future of our organizations from cyber threats.