-----Original Message-----
From: Susie Cordell <Susie.Cordell[redacted]>
To: andra.gyor[redacted] <andra.gyor[redacted]>; moesefamily[redacted] <moesefamily[redacted]>; A.J. Stephani <ajstephani[redacted]>
Cc: Debbie Vicknair <Debbie.Vicknair[redacted]>
Sent: Tue, Feb 11, 2020 9:10 am
Subject: FW: Hacked emails Unit 164

Hi Andra,

I received a copy of your email. I am so sorry that you have been spoofed. This is not uncommon – and it is not specific to ACBL email. Just as an FYI – the outside world cannot get information from our ACBL site – you have to log on with a Member ID. I just logged on to ACBL.org and tried to get to clubs, units, etc. to verify before sending this email. If, however, you find that you or someone else can access your info without logging in, please let me know right away. We take all of these instances serious and work hard to keep our site safe.

FYI - just because a *phishing email* lands in your inbox, it doesn't mean your computer is infected with a virus or malware. ... Phishers might send *emails* to thousands of addresses every day, and if you reply to one of their messages, it confirms your *email* address is live. This makes you even more of a target. We appreciate you alerting us and helping to keep our network, and our people, safe from cyber threats.

Phishing" is the most common type of cyber-attack that affects organizations like ours. Phishing attacks can take many forms, but they all share a common goal – getting you to share sensitive information such as login credentials, credit card information, or bank account details.

The particular email we were made aware of this time is a form of 'spoofing'. Spoofing is when someone makes an email appear as though it was sent from somewhere it wasn't, such as your email address. This is often used in 'whaling' efforts. Whaling is a popular ploy aimed at getting you to transfer money or send sensitive information to an attacker via email by impersonating a real company executive or representative. Using a fake domain that appears similar to ours, they look like normal emails from a high-level official of the company, typically members of the Executive Team and/or Board Members.

Although we maintain controls to help protect our networks and computers from cyber threats, **we rely on you to be our first line of defense.**

Phishing and How You Can Help
"Phishing" is the most common type of cyber-attack that affects organizations like ours. Phishing attacks can take many forms, but they all share a common goal – getting you to share sensitive information such as login credentials, credit card information, or bank account details.

Outlined below are a few different types of phishing attacks to watch out for:

- **Phishing:** In this type of attack, hackers impersonate a real company to obtain your login credentials. You may receive an e-mail asking you to verify your account details with a link that takes you to an imposter login screen that delivers your information directly to the attackers.
- **Spear Phishing**: Spear phishing is a more sophisticated phishing attack that includes customized information that makes the attacker seem like a legitimate source. They may use your name and phone number and refer to ACBL in the e-mail to trick you into thinking they have a connection to you, making you more likely to click a link or attachment that they provide.
- **Whaling:** Whaling is a popular ploy aimed at getting you to transfer money or send sensitive information to an attacker via email by impersonating a real company executive. Using a fake domain that appears similar to ours, they look like normal emails from a high-level official of the company, typically members of the Executive Team, and ask you for sensitive information (including usernames and passwords).
- **Shared Document Phishing:** You may receive an e-mail that appears to come from file-sharing sites like Dropbox or Google Drive alerting you that a document has been shared with you. The link provided in these e-mails will take you to a fake login page that mimics the real login page and will steal your account credentials.

What You Can Do
To avoid these phishing schemes, please observe the following email best practices:

1. **Do not click on links or attachments** from senders that you do not recognize. Be especially wary of .zip or other compressed or executable file types.
2. **Do not provide sensitive personal information** (like usernames and passwords) over email.
3. Watch for email senders that use **suspicious or misleading domain names**.
4. **Inspect URLs carefully** to make sure they're legitimate and not imposter sites.
5. **Do not try to open any shared document** that you're not expecting to receive.
6. If you can't tell if an email is legitimate or not, please **DO NOT RESPOND**
7. Be especially **cautious when opening attachments or clicking links** if you receive an email containing a warning banner indicating that it originated from an external source.

Please let us know if you have any questions. You may want to send this email on to your board members.

Sincerely,

Susie Cordell
Director of Information Technology
Office: 662-796-7234
Cell: 901-490-9736
www.acbl.org
American Contract Bridge League