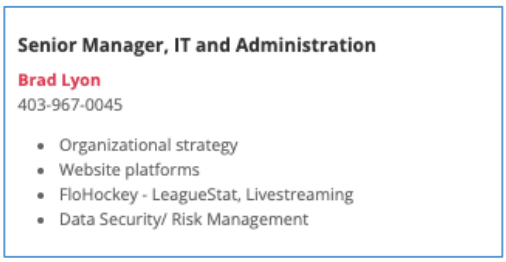
integrity.
community.
collaboration.
innovation.
passion.

Dealing with Phishing

Some Cyber Security Best Practices and Tips

Utilize and safeguard organization email accounts:

1. Create organizational email addresses for key volunteer, executive, staff and/ or board positions rather than using personal emails. This could be an organizational URL based on your website address (such as president@hockeyalberta.ca), or something within an existing email provider (such as president.hockeyalberta@gmail.com).
2. If choosing to set up emails within an existing provider, choose an email provider that offers robust security features, such as encryption and advanced spam filters.
3. When listing individual contact information on your website, post the person's name and/ or position, and hyperlink the email address within the name. Don't display the actual email address. As shown here on the HA website, to get the email address, you actually have to click on the name.



4. Use strong, unique passwords for your email accounts. Generally, it is recommended passwords should be a minimum of 10-12 characters with letters (upper and lower case), numbers and symbols included. Random phrases are also recommended.
5. Require regular password updates. Set reminders to change passwords periodically (at least annually, and preferably more often).
6. Restrict access to email accounts to only those who need it and avoid sharing login credentials.
7. Enable two-factor authentication. This adds an extra layer of security by requiring a second form of verification, such as a code sent to a mobile device.
8. Keep software updated. Ensure that all devices used to access email are running the latest security updates. Also, if accessing email on a mobile device, use the email platform's app, rather than a generic mail server. For example, if using gmail on an IPhone, download the gmail app, don't use the default Apple Mail app.
9. Ensure dormant accounts are deleted or disabled, and cut off access for those people who have left your organization. Also ensure that any forwarding is turned off.
10. Establish clear security policies for email usage, including guidelines for password management, account access, and handling suspicious emails. Policies should also include expectations of what an individual will do if something happens involving their organizational email.

Establish protocols for sending emails:

1. Use a clear and concise subject line that accurately reflects the content of the email. This helps recipients understand the purpose of the email and reduces the likelihood of it being marked as spam.
2. If you need to include file(s) in the email, please ensure the file is named to reflect its content. If adding an attachment to your email, provide a brief explanation about the attachment to help clarify for the recipient that it is legitimate.
3. It is a good idea not to share files via links in Microsoft Sharepoint/ OneDrive or Google Drive. Shared links are a common way that bad actors gain access to your email and potentially your computer system.

4. If sending a mass email, use a third-party mass email platform. There are several reputable companies, and they have safeguards built in to help ensure the security of the email.

5. If you plan to send regular emails to your members, provide that information at the beginning of the season, so they know when they can expect to have communication updates from you.

How to evaluate if a message is legitimate:

Bad actors want their message to appear to come from a specific individual who is known to you. The email will list the name and possibly the title. It might also display an email address. Common phishing emails ask if you are busy, or if you can purchase gift cards for someone. But they are also becoming more creative (or brazen) in trying to convince you to carry out an action.

Read each message carefully, especially if you are being asked to click on an attachment or a link or to send someone money or gift cards. Make sure the email seems legitimate before clicking on anything. You can use the following criteria in your evaluation:

1. **Suspicious Sender**: Check the sender's email address carefully. Phishing emails often come from addresses that look similar to legitimate ones but have slight variations (.com vs .ca, or a dash in an address rather than a period etc)
2. **Generic Greetings**: Be cautious of emails that use generic greetings like "Dear Customer" instead of your name. Legitimate organizations usually personalize their emails.
3. **Urgent or Threatening Language**: Phishing emails often create a sense of urgency or fear, urging you to act quickly to avoid negative consequences.
4. **Unsolicited Attachments**: Be wary of unexpected attachments, especially if they come from unknown senders. These attachments could contain malware.
5. **Links to Fake Websites**: Hover over any links in the email without clicking. Check if the URL looks legitimate and matches the organization's official website.
6. **Requests for Personal Information**: Legitimate organizations will never ask for sensitive information like passwords, SIN, or credit card details via email.
7. **Spelling and Grammar Errors**: Many phishing emails contain noticeable spelling and grammar mistakes. Legitimate organizations usually proofread their communications. Please note that, due to the growth of AI, improvements are occurring in this area and spelling and grammar is improving even in phishing messages.
8. **Unusual Requests**: Be cautious of emails asking you to perform unusual actions, such as transferring money or providing confidential information.
9. **Too Good to Be True Offers**: Be skeptical of emails offering deals or prizes that seem too good to be true. These are often used to lure victims into providing personal information.
10. **Mismatched URLs**: Check if the URLs in the email match the official website of the organization. Phishing emails often use URLs that look similar but have slight differences.

If you receive a phishing message:

If you believe you have received a phishing email, take immediate action to protect yourself and your information. Here are the steps you should follow:

1. Do not respond to the email or click on any links or attachments.
2. Report the email**.** Most email providers have a feature to report phishing emails. Use this feature to help prevent others from falling victim to the same scam.

3. Take a screenshot of the message**.** This can help your IT provider if an investigation is undertaken.
4. Delete the email**.** After reporting, delete the phishing email from your inbox and your trash folder to ensure it is completely removed.
5. Change your password. If you have clicked on any links or provided any information, immediately change the password for your email and any other accounts that may be affected.
6. **If** you haven't already, enable **two-factor or multi-factor authentication** on your accounts for an added layer of security.
7. Use your antivirus software to run a full security scan on your device to check for any malware or viruses that may have been installed.
8. Keep an eye on your bank accounts, credit cards, and other sensitive accounts for any unusual activity. Report any suspicious transactions to your financial institution immediately.
9. Learn more about phishing scams and how to recognize them. Share this information with friends, family, and colleagues to help protect them as well.

If you are "sending" phishing messages:

If you become aware that someone is sending fake emails using your name, or your association's email accounts, it's important to take immediate action to mitigate any potential damage. Here are the steps you should follow:

1. Inform the recipients as soon as possible that the email they received was a phishing attempt. Advise them not to click on any links or open any attachments. You can also post a message to your website and/ or social media channels alerting people about what has happened.
2. If you have an IT provider, report the phishing email to them. They can help assess the situation and take necessary actions to protect your organization's network.
3. Change passwords for all organizational emails and any other accounts that may be affected. Use strong, unique passwords to enhance security.
4. **Carry out steps 6 through 9 listed in the previous section on what to do if you receive a phishing email.**

If you have questions on IT and/ or cybersecurity:

Brad Lyon,
Senior Manager, IT and Administration
Phone: 403-967-0045
Email: blyon@hockeyalberta.ca