FUTALEUFU MUSINGS

SEARCH FUND INVESTING. OLD SCHOOL.

Internet Security: A Sad Search Fund Story

A few years ago, we had an investment that was doing quite well. So much so they were in a sale process where we expected a 3.7x MOIC. Halfway into the sale process, they were hacked and ransomed and the perpetrators got sensitive customer information. The sale process fell apart. Two years later the company was sold for 0.8x MOIC, and the entrepreneurs received nothing. Protecting your networks is not just for Marriott, JP Morgan, and Home Depot. It happens to search fund companies as well.

You might be watchful and knowledgeable about internet security, but can you safely say that about every employee who works for you? Unless you can say that with certainty, you are vulnerable.

Here is a YouTube video that can be easily watched at 2x speed. The video summarizes the most essential things you should do if you want to avoid what happened to the search fund company we just described.

In addition, we strongly encourage you to share this musing with your team.

Phishing

Phishing and spear phishing are malicious techniques used to deceive individuals into revealing sensitive information or installing malware.

To safeguard against these threats:

- Examine the email sender’s identity. Verify the domain.
- Be wary of grammatical errors in the message.
- Hover over links to check for suspicious URLs and manually type them when in doubt.

Email Attachments

Email attachments are a common method for spreading malware. Opening an attachment from an unverified source can quickly lead to a computer infection.

To safeguard against these threats:

- Avoid opening and saving attachments from unknown senders.

- If an attachment appears suspicious, refrain from opening or saving it.

Spam Protection

Protecting against spam emails is essential for online security.

To safeguard against these threats:

- Maintain the rule of never opening, clicking, or responding to spam emails.

- Be cautious when sharing your email address on websites.

- Add special breaks to your email address when sharing with others. For example, instead of using sarahjones@partners.com, use sarahjones@ partners (dot)com.

- Consider using third-party spam blockers and filters.

Passwords

Protecting your online accounts and personal information is crucial.

To safeguard against these threats:

- Unique Passwords: Always use unique and strong passwords for each of your accounts. Avoid using the same password on multiple websites.

- Two-Factor Authentication (2FA): Whenever possible, activate 2FA for your online accounts.

- Security Questions: When setting up security questions, opt for answers that cannot be guessed easily or found through public information. Through social media and data scrapes, your first car, your mother's maiden name, and the name of your pet is easily discovered. One way past this is to not use the actual names as your security answer.

- Password Changes: In the event of a data breach or any suspicious activity, change your passwords and security questions immediately.

Malware

Malware poses a significant threat, especially on Windows systems. Malware can infect your devices through various means, such as clicking on malicious links, plugging in unknown flash drives, and downloading software from untrusted websites or email attachments.

To safeguard against these threats:

- Endpoint Security: Install reliable security software on your devices to detect and prevent malware infections.

- Device Vigilance: Be cautious about what you plug into your devices, particularly when it comes to unknown or untrusted flash drives.

- Cybersecurity Awareness: Stay informed and educate yourself about the latest malware threats and best practices for online security.

Public Wi-Fi

Public Wi-Fi networks are often insecure, and it's essential to consider them as potentially compromised. As well, it is a common tactic to set up fake Wi-Fi networks – for example at the bagel shop a hacker will create a network called "Bagel wifi," which you will assume is managed by the shop.

When using public Wi-Fi:

- Verify Wi-Fi Network: Confirm the legitimacy of the Wi-Fi network with business owners or staff before connecting.

- Assume that public Wi-Fi networks may be compromised and never conduct sensitive activities like online banking or social networking using these networks.

- Anti-Malware Software: Use anti-malware and security software on your devices to add an extra layer of protection against potential threats while on public Wi-Fi.

Your Partners at FTF

David Dodson
Susan Pohlmeyer
Jason Jackson

Samuel Spar
Kirstin Siegrist
Andrea Chiang