Cybersecurity case study

Meet Bob

Bob is a financial professional who manages his own advising practice. One morning, he receives the following email. Bob clicks **"SIGN IN TO MICROSOFT ACCOUNT PORTAL"** to prevent account malfunctions as prompted by the email.

From: MSTeam-Outlook Message Center <no-reply@office365protectionservices.co.uk>
Sent:
To: Bob Smith Bob.Smith@Company.com
Subject: Account Verification

> This mail is from a trusted sender.

o✓ Outlook

We're having trouble verifying your account: Bob.Smith@Company.com   on our server, most Features will be turned off.
To help prevent malfunctions, please log into your account portal to verify your account.

SIGN IN TO MICROSOFT ACCOUNT PORTAL

Note: Outlook will automatically fix your account after this process on the Microsoft server and all account Features will be turned back on.
Thanks for using office365 , we hope to continue serving you.

Microsoft Corporation
One-Microsoft Way Redmond
WA, 98052
All Rights Reserved | Acceptable Use Policy | Privacy Notice

The next day, Bob tries to log in to Outlook but is unable to access his account. He contacts Microsoft and learns that his account password and multifactor authentication settings were updated yesterday. At the same time, clients begin to call Bob's office, reporting strange communications from Bob's email address.

Bob immediately reports this phishing incident to the proper authorities. Over the next week, he works with Microsoft to regain access to his account, communicate with impacted clients, and ensure no other business areas were impacted by the security breach.

What is phishing and how does it occur?

Phishing is the most common type of social engineering, accounting for more than 90% of successful cyberattacks. These attacks include the following elements.

Element	Typically looks like	In Bob's Case
Bait	fake emails or messages sent by threat actors	Bob receives an **"Account Verification"** email
Hook	realistic messages that create urgency	Bob is prompted to **"verify"** his account to avoid losing access to certain features
Trap	an action such as clicking a link or opening an attachment, that collects information or installs malware	Bob clicks **"SIGN IN TO MICROSOFT ACCOUNT PORTAL"**

Consequences of a phishing attack

There's a lot at stake when it comes to cybersecurity attacks. Consider the following consequences Bob may face as a result of this phishing attack.

- **Financial losses:** Several costs were incurred during the remediation and restoration process. Bob also lost potential revenue due to operational disruptions
- **Diminished client trust:** Clients who received communications from Bob's email during the phishing attack feel less confident in his ability to protect their information and investments.
- **Operational disruptions:** While the issue was being resolved, Bob and his team lost access to their business emails. During this time, nearly all business operations were halted.
- **Regulatory consequences:** Following a regulatory investigation, Bob was required to make certain cybersecurity improvements to his business and pay a fine.

Preventing future attacks

To avoid future attacks, Bob should use the following strategies and tools:

- **Go slow.** When addressing potential phishing attempts, carefully review before opening attachments or clicking on links.
- **Update software.** Apply "patches" (software updates) as soon as they become available to ensure security.
- **Use filters.** Email filters and anti-phishing software blocks emails with malware, spyware, phishing attempts.
- **Employ multifactor authentication.** Users are required to verify their identity in more than one method such as passwords, phones/tokens, or biometrics.
- **Plan ahead.** Establish a cybersecurity incident response plan to quickly respond to future incidents.

At MassMutual Ascend, we have educational tools and resources to help facilitate conversations with your clients about obstacles they may face as they plan ahead. The Beyond Annuities value-add program was designed to help your clients as they plan for a secure financial future. **Learn more and find additional resources at MMAscendConnect.com/BeyondAnnuities.**

For additional cybersecurity resources, visit the Cybersecurity Infrastructure & Security Agency at CISA.gov.

∴ MassMutual Ascend