INVESTIGATING PHISHING EMAILS

If your organization is notified that emails are being sent that appear to come from you or an employee of your organization, the following process can be useful in determining if the email is spoofed or if you have a compromised email account.

Investigate if **Spoofed or Compromised**

- Determine if the emails are being spoofed to look like your user or if they are actually being sent from your system.
- Sometime the from address is wrong or slightly varied from your actual domain.
    - chad@sbscyber.com vs chad@sbccyber.com
- Inspecting one of the reported emails will help. You'll need a copy of the email, a forward will lose the needed header information. Ask your employee to go to File – Save As and save the email to their desktop using the Outlook Message Format. They can attach that to an email and sent it to you. Then you can examine the header information and see the originating server IP and SPF record information. You can also look for signs of sent items from the users email account. But keep in mind, hackers generally try to delete evidence, such as sent items and draft files.
- Resulting answer of your investigation should be 1) Spoofed or 2) Compromised.

If spoofed, you can report it as phishing to the following:

- https://www.us-cert.gov/report-phishing
- https://www.antiphishing.org/report-phishing/

If compromised, its critical to figure out HOW and this will help you figure out if your computer is compromised or if they just stole your password. To investigate this:

- Log into your email system and review user authentication logs. If the computer is also compromised, the IP addresses should match that of your office. Otherwise unusual logins should show during the time of suspected compromise from other states or countries. A common issue we see in systems such as Office 365 is that the logging was not turned on and there isn't evidence to investigate. See the Microsoft Office 365 Security Suggestions to improve things like logging.
- You can also scan the computer for malicious software. But do keep in mind that new malware might be undetectable to your standard scanning tools.
- Resulting answer from your investigation should be 1) Remotely Access or 2) Compromised workstation.

Cleanup

- Figuring out how the account was compromised and if the user's workstation is infected is very important. If the workstation is infected with malware, things like changing the password won't help as the hackers will see the new password being entered from the compromised system they are monitoring. It's more likely they are remotely accessing the email account after stealing the password but workstation compromises do frequency happen as well.
- Wipe any computer clean and reload it.
- Changing passwords and enabling Multi-factor Authentication will help get control back from the compromised account.
- See the attached Microsoft Office 365 Security Suggestions for additional best practices.

MICROSOFT OFFICE 365
SECURITY SUGGESTIONS

The following suggestions are intended to provide ideas on improving the overall security of your instance of Microsoft Office 365. Some of these suggestions will also work on more traditional Microsoft Exchange Systems as well. The list is not intended to be comprehensive, there are other controls not included here. As an example, Microsoft has a tool that will evaluate your Office 365 risks and provide control suggestions. You can find that tool here: https://securescore.office.com. The Center for Internet Security (CIS) also provides system hardening guidelines and is a great resource in improving security: www.cisecurity.org.

Suggested Controls:

- ✓ Secure user accounts
  - Enable multi-factor authentication (MFA) for all accounts
  - Enable strong password settings
    - We encourage 14 characters, complex, changed every 90 days
  - Disable user's ability to authorize third-party app's access to O365 information
    - Prevents users from accidentally allowing malicious applications that, once authorized, can access user emails and data, even after their credentials are changed
  - Restrict access to specific devices or locations (Conditional Access)
    - IP whitelist
    - AD or Azure AD domain-joined machines only
    - Devices enrolled in mobile device management (MDM)
- ✓ Enable Office 365 audit logging in the Security & Compliance Center
- ✓ Enable alert policies in the Security & Compliance Center (examples below)
  - Alert when a user or admin creates an email forwarding/redirect rule
  - Alert when an admin starts or exports an eDiscovery search
  - Alert when a user is assigned elevated Exchange admin permissions
  - Alert when a malware campaign is detected, or a large amount of email is reported as phishing
  - Alert when a user externally shares or deletes a large number of files in a short period of time
  - Alert when an external user performs a large number of activities on files shared with them
- ✓ Enable alert policies in Office 365 Cloud App Security (examples below)
  - Impossible travel
  - Activity from infrequent country
  - Activity from known anonymous IP addresses (proxy servers)
  - Activity from suspicious IP addresses
  - Unusual user or administrative activities
  - Multiple failed login attempts

- ✓ Configure threat management policies in the Security & Compliance Center
  - Anti-spam rules
    - Enabled SPF hard-fail and filtering email by language/geo IP
    - Increase bulk mail sensitivity
  - Anti-malware rules
  - Advanced threat protection (ATP) anti-phishing rules
    - Enable protection for all domains / users
    - Enable safety tips
  - ATP safe attachments and Safe Links rules
- ✓ Prevent data loss
  - Data loss prevention (DLP) rules in the Security & Compliance Center
    - Alerts and/or prevents emailing and sharing of documents containing sensitive information
  - Mail flow rules in the Exchange Admin Center
    - Create a rule to prevent external email forwarding/redirection (you can whitelist specific addresses)
  - Data retention rules in the Security & Compliance Center
    - Preserve deleted email and files for X number of days
  - Restrict external sharing from OneDrive, SharePoint and Exchange
    - Disable anonymous external sharing, limit sharing to specific external domains, or disable it entirely
    - Require external shares to expire after X days or prevent external editors from sharing with additional users
  - Restrict guest access to Skype for Business and Teams to specific domains
  - Encrypt sensitive emails and documents using Office365 Message Encryption/Azure Information Protection
- ✓ Improve email deliverability and help external recipients determine if emails were legitimately sent by your organization
  - Sender Policy Framework (SPF)
    - DNS record instructs recipient servers what IP addresses legitimate email can originate from
  - Domain Keys Identified Mail (DKIM)
    - Enable DKIM signing the Security & Compliance Center
    - DNS record gives recipient servers a key that all legitimately received email should be signed by (enforcement requires a DMARC record)
  - Domain Message Authentication Reporting & Conformance (DMARC)
    - Requires both SPF and DKIM to be properly configured
    - DNS record instructs recipient servers how to handle spoofed email purporting to be from your organization and how such incidents can be reported to you
  - Verify these DNS records exist and are following RFCs (internet standards) by using SPF/DKIM/DMARC record checkers
- ✓ User education and notifications
  - Enable email banners for messages originating from outside the organization
  - Train users on security controls and phishing scenarios using a tool like KnowBe4