7 Questions to Ask Now to Protect Your Workforce & Prevent Wire Fraud

Webinar

{B(W)} CYBER SERVICES

Presenters

MICHAEL BRICE

FOUNDER OF BW Cyber Services

28 years experience providing technology, security, and related cybersecurity consulting solutions for multiple industries, including deep commercial and military experience in the financial services industry as well as classified government operations. Received specialized training by the National Security Agency in Signals Intelligence. Former Marine Officer – served in the 1st Gulf War.

ANTHONY D. MASCIA

MANAGING PARTNER EFSI

Co-founder and partner of Essential Fund Services International, LLC (“EFSI”) and oversees EFSI’s business development and marketing. Anthony began his professional career as a trader and member of the New York Board of Trade in 1999. As a member of the New York Board of Trade (NYBOT) & Intercontinental Exchange (ICE).

Back to the Basics

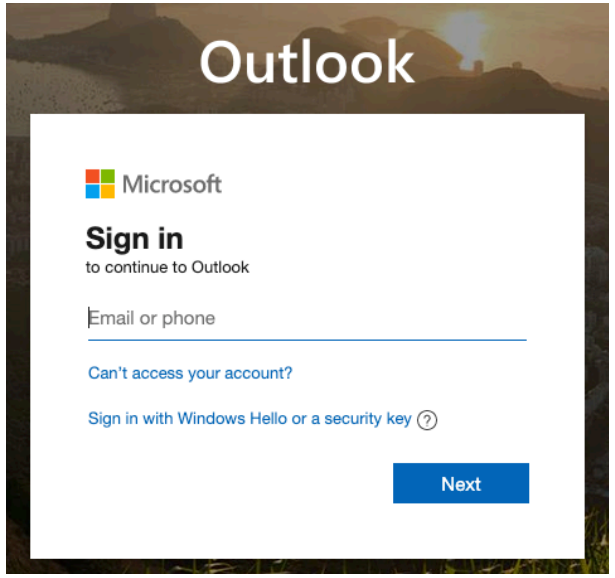
- What we've learned doing Incident Response and Forensics in the financial services industry – primarily asset management
- KISS - Vast majority of breaches are due to simple control lapses
  - Easy fixes
  - Not costly
  - Trust but verify
  - Education is critical

Current Situation

The Attack

A clever phishing e-mail that an employee or investor clicks

The Prize



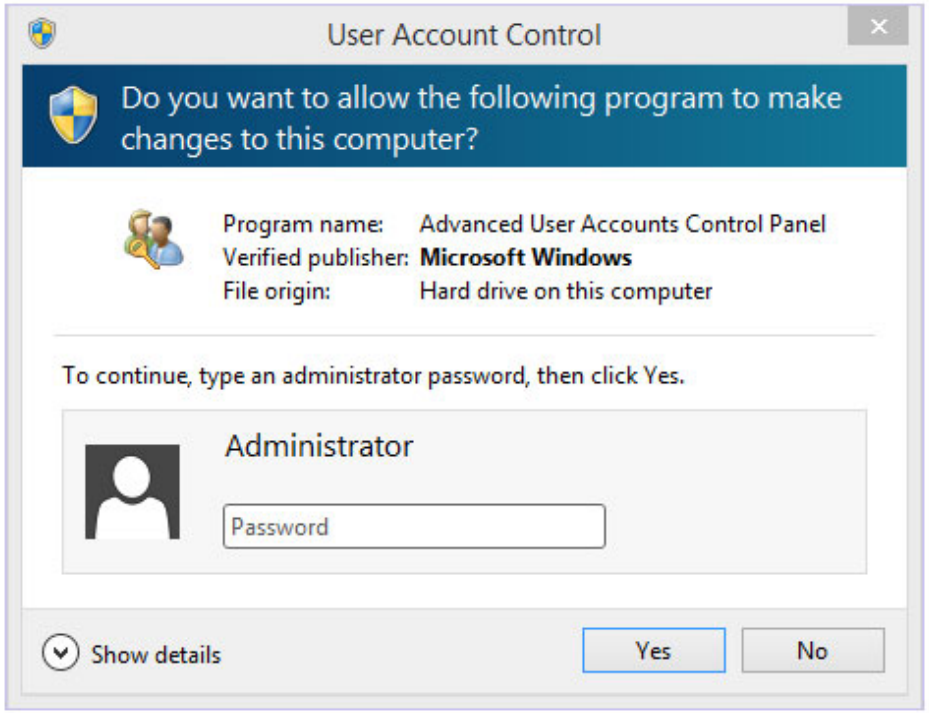
Redirection to a Credential Harvesting website (e.g., masquerading as Microsoft) to steal your login credentials

Financial Fraud

By secretly providing fraudulent wire instructions from a valid e-mail account (often for valid wires) – the criminal redirects the funds to a different bank account

1 Local Administrative Privileges

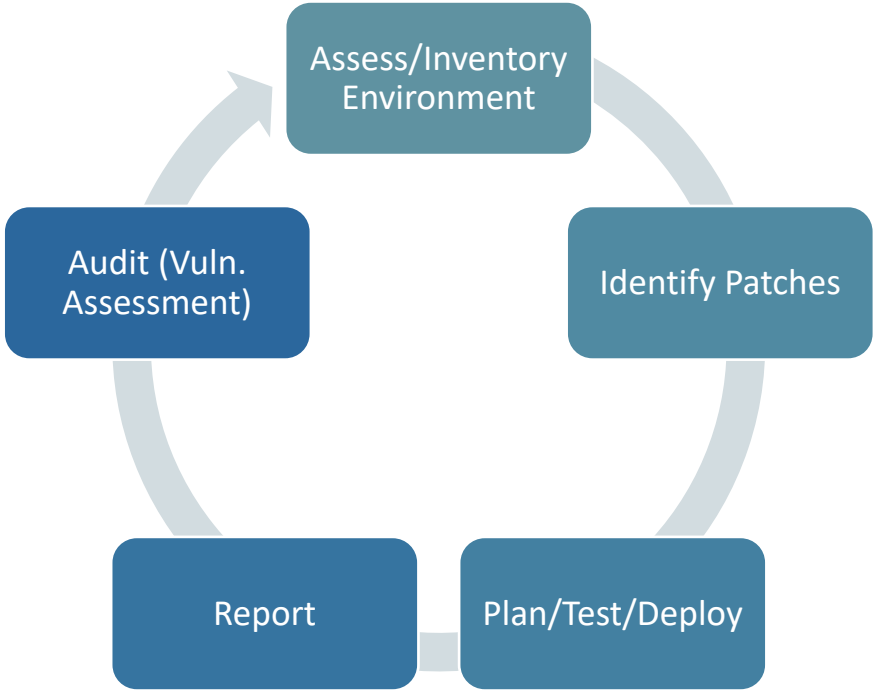
- Have you disabled Local Admin Privileges on all user's remote PCs?
  - Strongly recommend not allowing business use of non-company issued PCs.



Most organizations often do not disable Local Admin privileges – however, most users absolutely do not need this capability

2 Software Patching & Anti-Virus

- Are remote user's PCs still being patched, and are A/V definitions being updated and PCs scanned per policy?

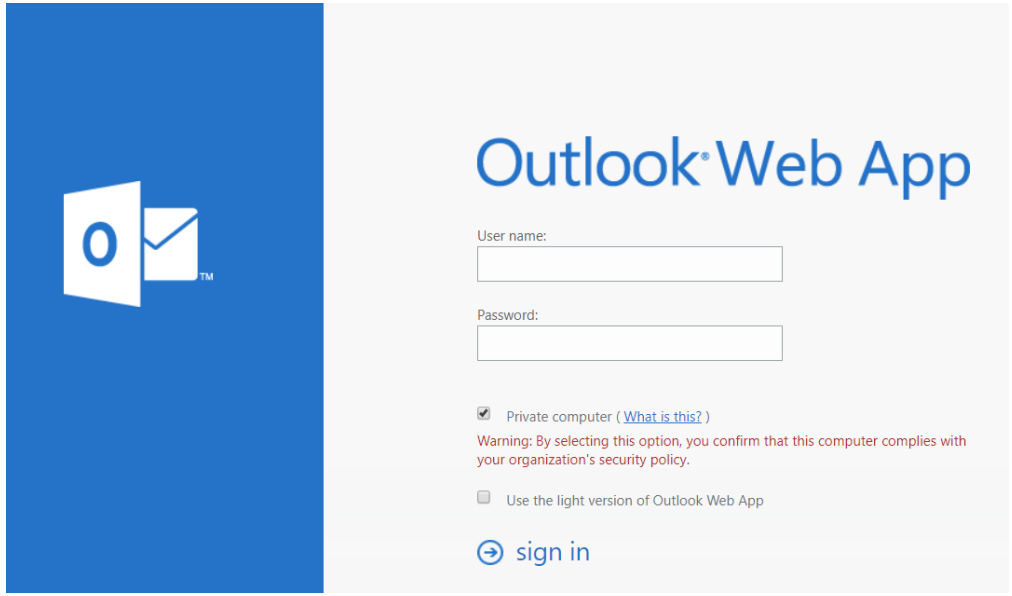


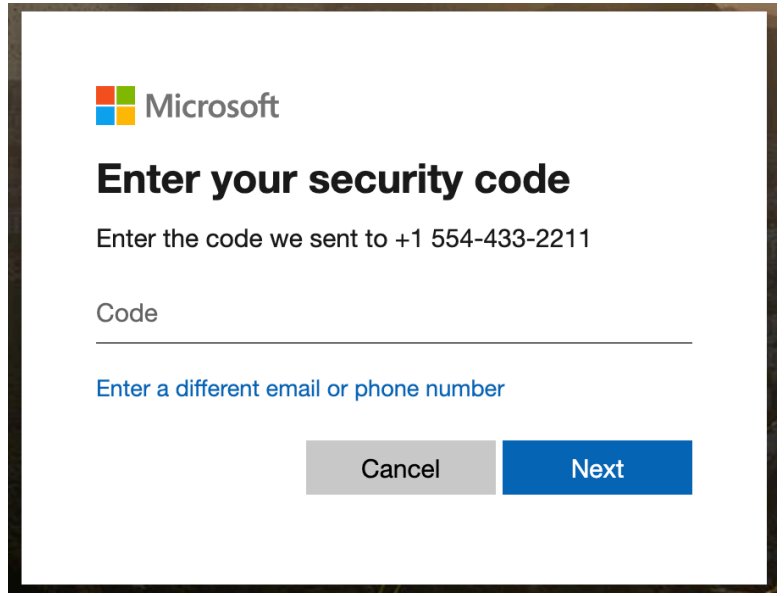
Patch Management Process

While local patching/upgrading (which is CRITICAL) is already a difficult task for IT; it's much more difficult to patch remote users

3 Outlook Web Access (OWA)

- For Microsoft users, is OWA enabled? If so, can you confirm that multifactor authentication (MFA) is configured as “Mandatory” (not just "Enabled”)?
  - Same with G-Suite & other cloud providers.

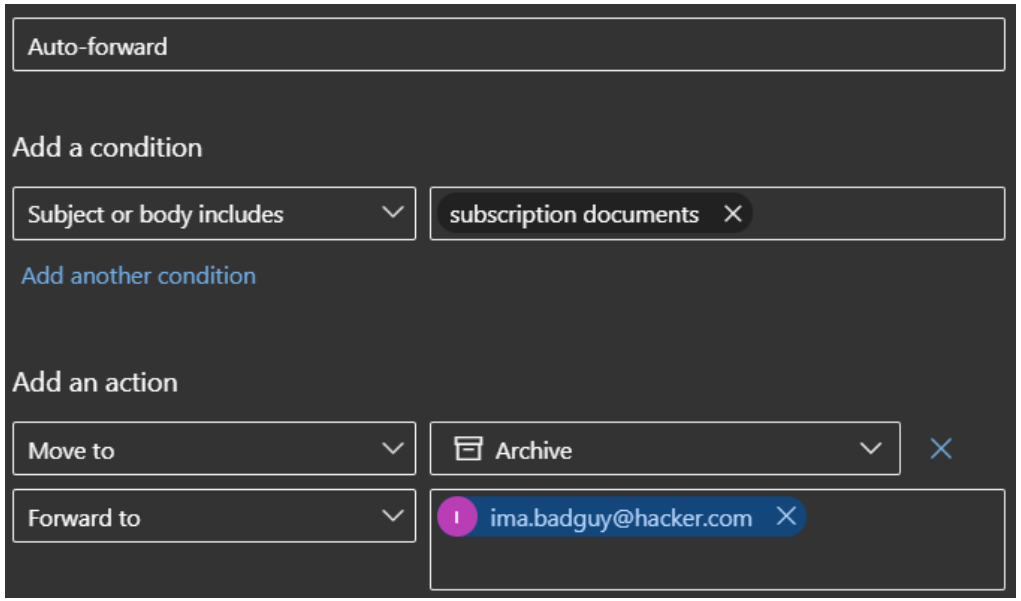




Without a doubt, this is the NUMBER ONE way criminals will break into an organization’s e-mail. ***LOCK IT DOWN w/MFA!***

4 Malicious Rules

- Can you perform a "rules" search on users' mailboxes to see if there are any auto-forward, auto-delete, or other anomalous rules (unknown to the user) that would be indicative of an ongoing breach?
  - Do you get and review alerts when a user creates a new rule?
  - Does your organization allow auto-forwarding out of the domain?

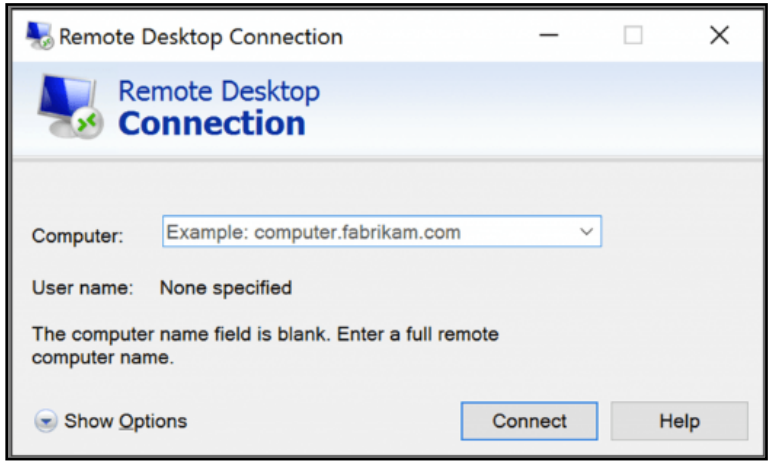


Example menu for email rules

Once in your e-mail, criminals will eventually set up rules to auto forward or auto delete e-mails (without the user's knowledge)

5 Remote Access

- Do you have MFA in place for all other means of remote access (e.g. VPN, RDP, LogMeIn, TeamViewer, etc.)?



TeamViewer

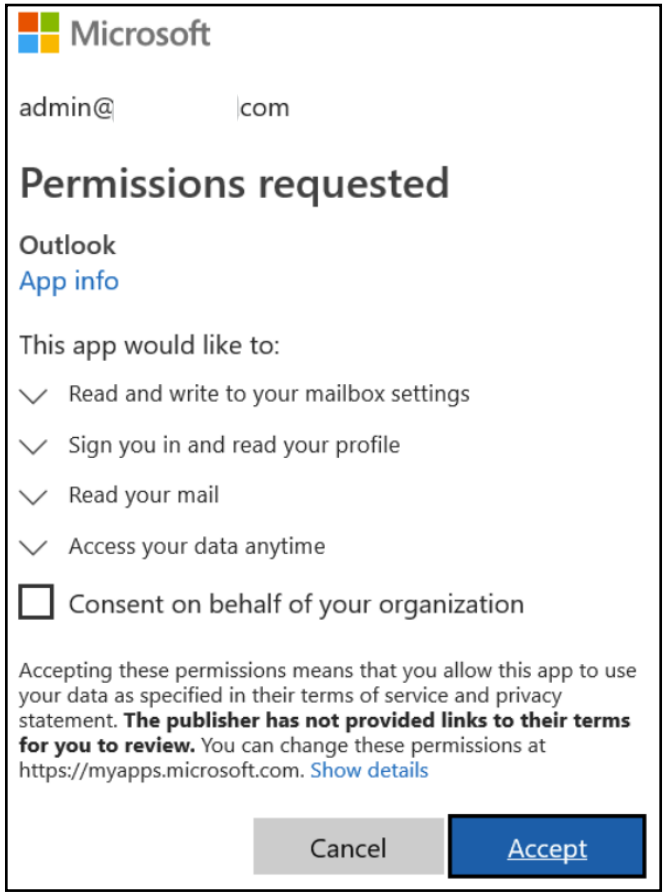
MYPC GoToMyPC

LogMeIn

Just like with OWA, it is CRITIAL that all forms of remote access to your network have MFA enabled. No exceptions!

6 MS Application Permissions

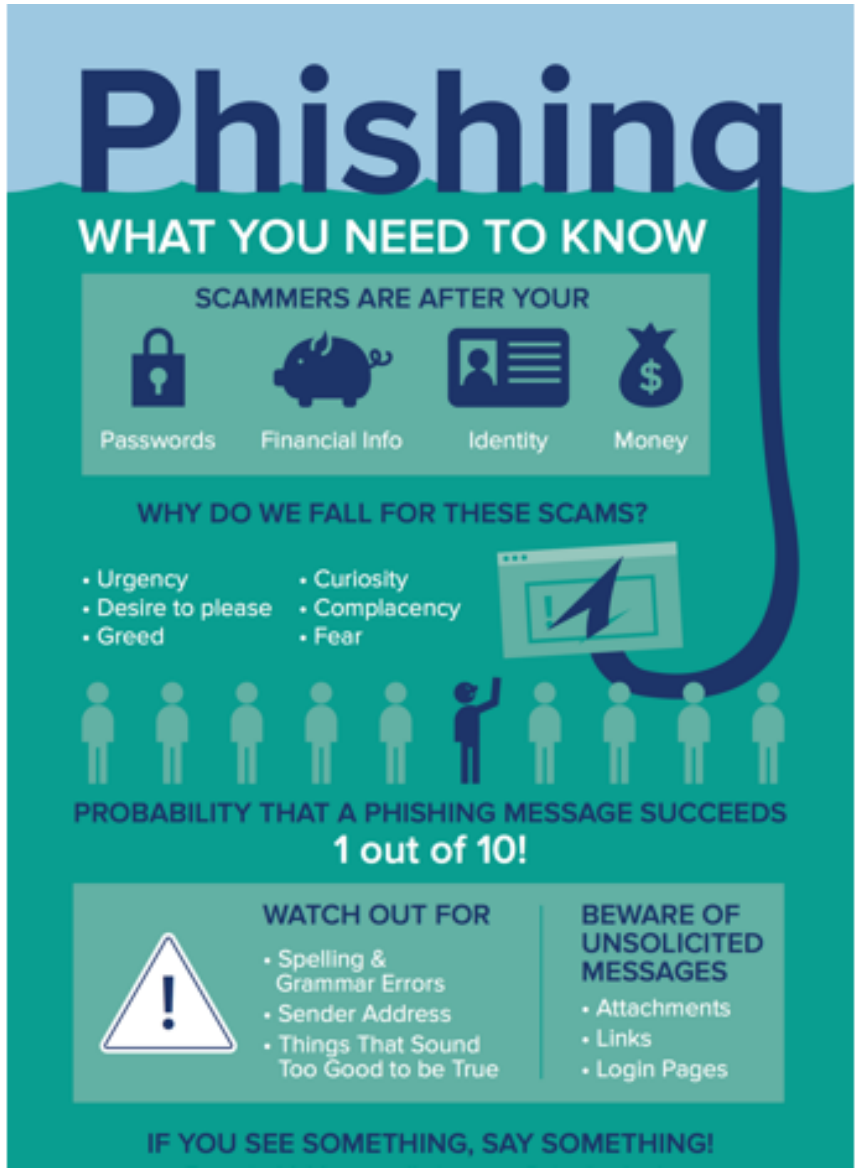
- For Microsoft users, can you confirm the applications that our users have granted permission to are valid?



This is attack method allows criminals to maintain access to your information even if you change the password or implement MFA.

7 Phishing Training

- Have you provided phishing training to our users recently? If so, was it custom tailored for the types of attacks that are being directed toward the asset management industry?
  - Have you tested your e-mail gateway against a TypoSquat (“impersonation”) attack?
    - e.g., `capitalheroes.com` can become: `caqitalheroes.com` (‘p’ to ‘q’)



TypoSquatting is a type of attack in which an e-mail domain is set up that is “almost” the same as your domain name.

The Bottom Line

- Unfortunately, often - it's not a matter of “If” but “When”…
- Verbal confirmation on all wires is critical
- It is critical your investors do the same
- The more you educate your investors, the better you are BOTH protected against wire fraud

QUESTIONS?

THANK YOU

{B(W)} CYBER SERVICES

(646) 779-8976 | info@bwcyberservices.com

www.bwcyberservices.com