UNDERSTANDING COVID-19 PHISHING ATTACKS

PROTECTING YOURSELF AND YOUR BUSINESS DATA

PRESENTED BY

Ntiva

Managed IT, Security, & Cloud Services

Attackers are looking to take advantage of the widespread COVID-19 news and perform various campaigns aimed at distributing malware and stealing user credentials.

Based on recent industry research, here are some specific examples of attacks your users may be exposed to:

SCAMS

A. Emails that are looking to sell coronavirus cures or face masks, or asking for investments in fake companies that claim to be developing vaccines.

B. Emails looking for donation requests to fake charities. There requests usually contain a Bitcoin wallet for donations.

MALWARE

A. Using phishing campaigns, malware can be distributed on user computers, and is aimed at stealing login credentials and company data.

B. Be on the lookout for documents that may appear to be from a trusted source (a client or co-worker). These documents can distribute malware when opened.

CREDENTIAL THEFT

A. Emails may claim to be from the CDC, and contain links to spoofed login pages. If clicked, these pages will ask for your username and password, attempting to steal Microsoft Exchange credentials.

WHAT CAN USERS DO TO PROTECT THEMSELVES?

1. Be suspicious of any emails attempting to get you to open an attachment or link.

Having a good email spam filtering solution in place to prevent these malicious emails from reaching the recipient is a good defense mechanism. However, while these solutions reduce the emails coming through, no mail filter will stop everything.

2. Never give out personal information.

A user should never make confidential entries through the links provided in emails. Never send an email with sensitive information to anyone. Make it a habit to check the address of the website. A secure website always starts with "https:"

3. Use caution opening emails from organizations you expect to hear from.

Make sure to check the actual sender's email address and domain name on every email you receive. Hover your mouse over any links to ensure they point to safe and trusted website.

WHAT CAN ORGANIZATIONS DO TO PROTECT USERS AND DATA?

1. Educate employees and conduct training sessions with phishing scenarios.

2. Keep all systems current with the latest security patches and updates.

3. Implement a security policy to address password expiration and complexity.

4. Implement Multi-Factor Authentication to protect access to applications and to the environment (such as a VPN).

5. Deploy a web content filtering solution to block malicious websites.

6. Deploy and email spam filtering solution to minimize the amount of phishing emails coming through.

7. Deploy an Endpoint Detection & Response (EDR) solution on every system to prevent malware from spreading into the environment.

Securing your users and your business requires a layered approach. Informed employees and properly secured systems are key when protecting your company from phishing attacks. If you need any assistance creating a strategic phishing prevention plan or with anything you see above, please reach out to us!

www.ntiva.com