Cyber Security Awareness: COVID-19

With the significant increase in employees now working remotely due to the Coronavirus (COVID-19), recent research by the Federal Bureau of Investigation (FBI) and Internet Crime Complaint Center (IC3) reveals a surge in cyber exploitation activity by threat actors. The two main trends are as follows:

Theft of Remote User Credentials

This crisis and the resulting social distancing and quarantine orders have led many organizations to promote a work from home policy to maintain business continuity. With a substantial shift to remote work, an exploitable opportunity for attackers was introduced.

Weaponized Email Attacks

There has been a double spike in incidents of phishing emails. Here are some examples:

- **Fake Emails:** Do not click unrecognized links or open attachments, especially from the Centers for Disease Control and Prevention (CDC) or other organizations claiming to offer information on the virus. Fraudsters use these links to deliver malware and steal sensitive data.

- **Counterfeit Treatments or Equipment:** Be cautious of anyone selling products that claim to prevent, treat, diagnose, or cure COVID-19, including sanitizing products and such personal protective equipment (PPE) as N95 respirator masks, goggles, full face shields, protective gowns, and gloves.

- **Stimulus Package:** Look out for phishing emails asking for verification of personal information to receive an economic stimulus check from the government. While economic stimulus checks have been a talking point, government agencies are not sending unsolicited emails requesting private information to send the money.

- **Fraudulent Charity Donations:** Be aware that there are fake emails circulating asking for donations, GoFundMe pages, etc. To make a charitable donation, go directly to the website of the charity of choice to submit payment. Always type the charity’s web address in the browser rather than click on an email link.

What You Can Do To Assist

Be extra vigilant. Be aware, not alarmed. There are steps and actions you can take to help:

- **Use Smart Password Strategy:** Ensure work and personal passwords are different, use complex passwords (e.g., letters, numbers, capitalizations, symbols), and change them regularly.
- **Utilize Multifactor Authentication**: While most work services have this feature enabled, set it up on personal accounts as well to improve security.
- **Avoid Pop-Ups, Unknown Emails, and Links**: Never click on links or download attachments from unknown emails.
- **Connect to Secure Wi-Fi:** Avoid public wi-fi, use a personal cellphone as a hotspot, or use a trusted wi-fi network (one that requires secure login and authentication).
- **Take a Deeper Look at Content:** Question whether or not the website link looks valid before clicking; verifying hyperlinks should be a habit.
- **Check Email Headers:** Confirm if you have given your email address to this company before, if you have an account with them, and whether the sender's identity matches the email's purpose.
- **Think About An Email's Purpose:** Businesses should not ask anyone to send passwords, login names, social security numbers, or other personal information via email.
- **Double-Check:** Confirm requests (e.g., someone requests that you wire them money) through an alternate communication.

For More Information on COVID-19

- **Medical Information:** For accurate, up-to-date information on COVID-19, go to www.cdc.gov, or consult your primary care physician.
- **Emergency Response:** For current information from the Federal Emergency Management Agency (FEMA), go to www.fema.gov; and for case counts, state information, and a chat feature, go to FEMA's National Business Emergency Operations Center Dashboard at https://fema.connectedsolutions.com/nbeoc.
- **Fake, Unapproved, or Counterfeit PPE:** For information from CDC, go to www.cdc.gov/niosh; there is also valuable information from the Food and Drug Administration (FDA) at www.fda.gov and the Environmental Protection Agency (EPA) at www.epa.gov.

If you have any questions, please reach out to your Dataprise team. We are here to help.

DATAPRISE