GCA Cybersecurity Toolkit Backgrounder: Prevent Phishing and Malware Toolbox

Over 90% of cyberattacks start with a phishing email. The intent of phishing is to trick people into believing they are dealing with a trustworthy entity so that sensitive information or access to money can be obtained by the criminal.

Phishing is the term generally associated with communication via email, smishing via text, and vishing via telephone. There are many different types of phishing; these are just a few:

- **Phishing**: This is generally untargeted. Mass emails are sent pretending to be from reputable organizations. They may relate to recent news stories, the tax year, or appear to come from common organizations used by many in the hope that some recipients will respond.
- **Spear-Phishing**: This is more targeted. The email will be designed to look like a person or organization known to the victim; some research needed on the intended target will have been done, often with a specific objective in mind.
- **Whaling**: This is highly targeted, often towards very senior figures within an organization. Reconnaissance will likely have been performed with the criminals having been tracking movements and collecting data for months before making a move. There will be a very specific objective in mind.

Once in your inbox, the attacker will hope that you click on a link or open the attachment which will facilitate the intended activity:

- **Malware**: A general term used for different types of malicious software:
  - **Virus**: Self-propagates and spreads via a host. It might attach itself to a legitimate program or file and activate when the program next runs.
  - **Worm**: Self-propagates and spreads on its own via network connections. For example, it might hide in an attachment and then email itself to all contacts in your email address book.
  - **Trojan**: Does not propagate; it disguises itself as a useful legitimate program (i.e., a screensaver) while causing damage in the background.

A **backdoor** might be created (a secret route into the computer for use later), data may be corrupted, and **spyware** (to track what you are doing and access personal information) or **ransomware** may be installed (locking your data and demanding a ransom be paid to retrieve it).

Phishing emails are NOT easy to spot

- They may look like they come from someone you know.
- They may have exactly the same email address as someone you know.

- They might mimic the logos and format of emails from well-known organizations.
- They might refer to recent 'headline news' or a job you've just done.
- The attacker might have called your company or checked online to personalize the email and to add further 'legitimacy.'

The attacker will do whatever they can to make their email appear genuine and enticing - they are very good at it.

The consequences are severe for individuals and businesses alike. Multiple studies show that small businesses are at high risk. At any one time over 60% of small businesses are likely to have suffered a cyberattack within the preceding year, with email being the primary initiator (or attack vector) used.

Anti-Virus Software (AV):
Helps protect against being infected; it works by checking for characteristics associated with known viruses (known as signatures) and if identified, blocks the virus and cleans up the file. New strains of viruses are continuously developed by the attackers to try and get around the AV software. When new viruses are released it takes a while for the characteristics to be identified and for the viruses to be blocked. Attacks that use new viruses for which no cure has yet been developed are known as 'zero day' attacks.
Anti-virus software may also look out for unusual operator behavior (known as heuristics); the AV learns your usual behavior patterns and becomes suspicious if something out of the ordinary takes place (i.e., logging onto a system at an unusual time).

It is important to keep anti-virus software up to date. New viruses are constantly being developed.

- *Ensure real-time anti-virus software is installed on all computers and mobile devices.*
- *Perform a periodic and regular scan of all your systems.*

Domain Name Filtering (DNS Filtering)

Terms and conditions apply when setting up new websites to ensure they are used for legitimate purposes - criminals ignore these and it is difficult to identify true intent until a website is operational.

- It is estimated that of the 200,000+ new domains registered daily across the globe, up to 70% may be intended for malicious activity.
    - https://unit42.paloaltonetworks.com/newly-registered-domains-malicious-abuse-by-bad-actors/

Many specialist cybersecurity companies monitor use of websites alongside other information to identify those that are operating suspiciously. Threat Intelligence (TI) is produced which, once analyzed, is used to confirm malicious intent. Domain Name Filtering will use this TI (from multiple sources) to block access to malicious websites, thereby preventing the intended harm from happening.

- **Quad9** is a DNS Filtering service developed by the Global Cyber Alliance in partnership with IBM and Packet Clearing House. It has 19 different threat intelligence feeds and blocks access to known malicious websites on a near real-time basis. It does this by refusing to convert and route traffic to the IP address associated with the website domain name typed into the browser. It may also block IP addresses your IoT devices or computers may be set (without your knowledge) to automatically connect to.

Domain Name Filtering can only block a website once a threshold of malicious activity is identified.

DNS: Domain Name System

- The Domain Name System (DNS) is the Internet's equivalent of a phone book.
- A unique website name or domain, in text format which we would understand (i.e., globalcyberalliance.org), is translated by Domain Name Servers into a unique set of numbers (the IP address - 192.124.249.5) which computers understand.
- New websites and domains are constantly created and registered by Domain Name Registrars which allocate and log the corresponding IP address (GoDaddy would be one example of a Domain Name Registrar).

The Registrars have to ensure that each website domain name and IP address is unique. Many fraudsters will try to use look-alike website domain names to trick victims into thinking they are connecting to a legitimate site. These sites may look like the real website name, but closer inspection may show differences (i.e., 'rn' may be used instead of 'm' in the website address).

Ad Blockers

Some adverts or messages that appear while browsing are useful; however, many are not and many contain malicious code. An ad blocker may be used to prevent advertisements appearing on webpages while browsing. They offer a further line of defense against attack.

Use the tools in the Prevent Phishing and Malware Toolbox to help protect yourself against falling victim to phishing and malware.

https://gcatoolkit.org/smallbusiness/prevent-phishing-and-malware/