GCA Cybersecurity Toolkit Backgrounder: Protect Your Email and Reputation Toolbox

Email is used extensively as the initiator for a cyberattack. It is extremely quick and inexpensive to send thousands of emails to unsuspecting recipients in the hope that at least some of them will be tricked into thinking they are genuine and click on the malicious website link or download the harmful attachment.

This could lead to your computer system being infected with some form of malware or ransomware, giving access to the criminal to steal valuable data or to transfer your money into fraudulent accounts. It could also allow the criminal to take control of your systems and manipulate your banking details, so customers make payments into other accounts thinking they are paying you.

The use of phishing emails is extremely effective for criminals – they can reach thousands of potential victims very quickly, but in order for them to be successful, the email needs to appear as if it has come from a legitimate source.

There are several ways the criminal might attempt to do this:

- **Display Name Spoofing**
  - Name displayed in the 'from field:' ***'Company'***
  - Email address: *'<person@yahoo.com>'*
    - *Hover over display name to check actual address before progressing.*
- **Look-Alike Domain Spoofing**
  - Name displayed in the 'from field:' ***'Company'***
  - Email address: *'<person@c**0rn**pany.com>'*
    - *Check the email address carefully before progressing.*
- **Domain Name Spoofing**
  - Name displayed in the 'from field:' ***'Company'***
  - Email address: *'<person**@company.com**>'*
    - *Use DMARC to protect against domain name spoofing.*

Even after checking and double-checking, always proceed with caution and use alternative means to check legitimacy if unsure (i.e., telephone the sender to check if they have actually sent the email).

The impact of having no defense against Domain Name Spoofing means:

- Attackers can pretend to be you or your supplier/customer to request payment or place orders.
- Attackers can also pretend to be others from within your own organization.

They may carry out:

- **CEO Fraud**, when an email is sent pretending to be the CEO or senior authorized person. They will often instruct a colleague that a payment needs to be made straight away.
    - *Instill a policy that it's good to double check - family businesses often operate on trust and little checks; attackers will take advantage of this.*
- **Business Email Compromise (BEC)** happens when an email is sent from an already compromised email account – sent 'from within the organization' or when the fraudulent email uses a legitimate domain name (domain name spoofing). These may be to suppliers or customers requesting payment, but to altered bank details. Because the attacker is 'within the organization' they will appear more genuine, with some authentication techniques ratifying the sender details making them more difficult to spot. The attacker may have been monitoring communications and been within the system for a while, so will appear very knowledgeable.
    - *Use DMARC to help prevent initial compromise, if domain name spoofing is used.*
    - *Utilize strong passwords and multi-factor authentication mechanisms to reduce chances of account compromise.*
    - *Check your email account settings regularly to ensure emails are not being forwarded to an unknown email address.*
    - *Have a policy to check all details for new suppliers and customers via at least two different methods. If any change is made, always check via a known alternate method (i.e., telephone via a known good number/switchboard, not just what might be contained within the signature as this may also have been changed).*

DMARC (Domain-based Message Authentication Reporting and Conformance)

A DMARC policy allows a sender to indicate that their messages are protected and tells the receiver what to do if one of the authentication methods passes or fails.

DMARC:

- Prevents an impersonator 'pretending to be you' in an email.
- Prevents you from receiving an email from an imposter.
- Provides insight into attempts to spam, phish, or spear-phish using your organization's email domain through reporting.
- Builds trust with customers and the supply chain.

But

- Both the sender and receiver must have a valid DMARC policy and DMARC verification in place for DMARC to be effective
- If the customer and supplier use DMARC, ***both*** are PROTECTED from email domain spoofing – if only one does, then neither are.
- What happens to the email once received depends on the senders DMARC policy setting

Use the tools in the Protect Your Email and Reputation Toolbox to find out more about DMARC and to configure it on your email domain.

https://gcatoolkit.org/smallbusiness/protect-your-email-and-reputation/