This is the third of a series of documents created by St. Andrew's parishioner Kelly Bourne, a retired computer security professional.

Cyber-safety Article #3 - Multi-Factor Authentication (MFA)

Traditionally online accounts and websites required that users entered an account ID, aka username, and a password to log in. This was relatively convenient but had a significant downside. If someone learned your username and password, they could log in and take control of the account. Multi-Factor Authentication (MFA) adds an additional security layer beyond knowing the password. With MFA in place even if someone knows your account ID and password then the account is still safe.

People may think that the chances of someone learning their passwords are minimal, but that isn't always the case. There are numerous ways that someone else can obtain them. Some ways are:

- A data breach at a website can reveal the usernames and passwords of all the site's users.
- Users can be tricked via social engineering into revealing their passwords.
- Malware (malicious software) known as a keystroke logger can be installed on a computer to capture all keyboard activity, including passwords.
- If a password that's reused for multiple websites or accounts becomes known, then all of the accounts using it are at risk.
- Passwords written on a Post-it and stuck to a keyboard or monitor provide little security.
- Passwords that can be easily guessed like "abcdefg", "123456", "password" and "qwerty" provide no security.
- Hackers have tools to try 'crack' passwords by making tens or hundreds of thousands of attempts to guess them.

Multi-Factor Authentication is one of the best ways users can protect their accounts. MFA is a generic term. If two different factors are required to protect to an account, then it's known as two-factor authentication (2FA). If three factors are used, then it's called three-factor authentication (3FA). The 'factor' referred to in MFA can be one of three forms:

- Something you know, for example a password, a PIN or the answer to a security question like "What elementary school did you attend?"
- Something you have, for example a cell phone, a security card or a security fob.
- Something you are, for example your fingerprints, your voice pattern, your retinal pattern or your facial features.

Even if you're not familiar with the terms you're almost certainly already using MFA. An extremely common MFA example is withdrawing cash from an ATM. You insert your card (something you have) into the machine and then enter your PIN (something you know) into a text field. This is an example of two-factor authentication (2FA).

Another example where users frequently encounter MFA is on their email accounts, e.g. Gmail, Outlook, Yahoo! Mail, etc. A typical scenario is to bring up the mail server's website in a browser and enter your email address (something you know) and password (something you know). A code, usually six digits, is sent to the smart phone (something you have) that's registered with that account. Once the correct code is entered into the login screen you can access the email account.

An example of a 3FA implementation that I am familiar with worked like this:

- Users logged into the network from their company issued laptop by entering their ID and password (Factor 1 - something you know).
- A two-digit number was display on the laptop's login screen (Factor 2 – something you have).
- That two-digit code had to be entered into a screen that came up on their company issued smart phone (Factor 2 – something you have).
- If the correct code was entered on the phone, then the camera on the phone had to be positioned so it could capture the image of the user's face (Factor 3 – something you are).

Only if the responses to all three factors were correct would the user be given access to the corporate network.

Examples of situations when MFA is typically utilized include:

- Accessing an employer's network when working remotely.
- Logging into social media accounts like Facebook, LinkedIn, Instagram and Twitter.
- Logging into websites that contain health information.
- Logging into email providers like Gmail, Outlook, ProtonMail and Yahoo! Mail.
- Logging into financial related accounts like bank accounts or investment accounts.
- Logging into government websites like Social Security, Medicaid, Medicare and the Internal Revenue Service.
- Logging into online games like Fortnite, Grand Theft Auto, Call of Duty and Street Fighter

MFA provides a significant improvement in security, but it isn't infallible. Some of MFA's weaknesses are described here:

- Some MFA setups allow users to choose whether codes should be sent to their smart phone or email account. If codes are sent to their email account and that account can be accessed by someone else, then MFA codes are compromised. Users should always choose to have codes sent to their smart phones.
- MFA bombing or MFA fatigue is a technique used to thwart MFA protection. Some MFA processes send a message to the user's smart phone and requires the user to click on an "Approved" option to get access to the account. A criminal who knows the account ID and password can repeatedly try to log into the account. Each attempt results in a text message being sent to the user's phone. The user may approve the request by accident or approve it to make the messages stop coming. In either event it grants access to the bad actor.
- If a user loses his phone or MFA fob, then MFA no longer provides any protection. Without the device the user won't be able to access her account.
- Bad actors can use social engineering to trick users and get around MFA. If they already know the password they can attempt to log into the account and call the user to obtain the MFA code that was sent to their phone.
- MFA takes a little more time and effort to log in an account. Some users aren't willing to put up with any inconvenience and never activate or eventually turn off MFA authentication. If MFA isn't enabled, then it can't provide any protection.

Some accounts require MFA. Other vendors or providers strongly recommend it be used, but don't require it. If you aren't currently using MFA to protect your accounts, then adding this additional layer of protection is a good idea. If should be set up for any account that involves money or confidential information.

- Kelly Bourne