Stop. Think. Connect.

Most human beings are lazy unless motivated by fear or greed. They need training on the need to “Stop and Think” before they “Connect”.

Educate Users to strengthen Passwords

With all the threats to the integrity of your sovereign business data, current password functionality is in need of an overhaul. The challenges are:

1. Staff members are under pressure to get more done. Using good passwords makes this harder. So staff need education on the dangers of using short, easy-to-guess passwords
2. Short passwords are terrifyingly easy to hack.

Any sysadmin knows the difficulty in getting all staff to use unique passwords of a decent quality. On most apps, your password is “hashed” or encrypted to make it difficult for hackers to crack.

The problem is that a modern high-end graphics card, for example, can decode password hashes by running more than 600 million hash operations per second.

A few of these cards arranged in an array can try every possible eight character password in about seven days.

And attackers have other, more advanced ways to crack hashes — with the right tools they can crack hundreds of passwords per hour.

Once a hacker gets a user’s password, they can use it to attempt access to the user’s online accounts — such as email or bank accounts. The big challenge is that most of us don’t follow password best practices.

A secure password should adhere to three basic rules:

- It should be long — at least 16 characters
- It should be complex — containing uppercase letters, lowercase letters, numbers, symbols, and spaces
- It should be unique — i.e. you only use it once.

Many password systems require users to create passwords of a certain length and complexity, but the resulting passwords are hard to remember and many users recycle the same password multiple times.

In fact, 54% of consumers use five or fewer passwords across their entire online life, while 22% use three or fewer.

With all these issues, combined with an increasing number of high-profile online data breaches, the public is losing faith in passwords. Nearly 70% of consumers report lacking a high degree of confidence that their passwords can adequately protect their online accounts — and they’re calling on online organisations to add another layer of security to the process.

Passwords are still an important security feature, despite their many problems. Check the strength of your passwords—make sure they are long, contain both caps, lowercase, symbols and numerals, and never repeat.

If you own an HP business PC, you can institute several layers of authentication at once — such as a fingerprint reader plus a password, or an iris scanner plus a smartcard reader. This is known as multi-factor authentication and is much more secure than any one method alone.

Many businesses use RSA Secure ID two-factor authentication to protect their staff notebooks and mobile devices.

RSA Secure ID tokens provide a code that changes daily and a pin number.

No system is perfectly secure. And the more secure the system, the more costs and negative impacts to useability.

Ask Evotec for an obligation-free analysis on your options to make your business more secure.

Beware fake invoice e-mails

There has been an increase in scam invoice e-mails being sent by internet fraudsters. Their MO is to send e-mails requesting payment of an outstanding invoice – usually between $1-3000 in value and contain an invoice as an attachment. The e-mails are plausible and are sent to actual e-mail addresses and include the name of the recipient.

Here’s three tips to avoid sponsoring crimeware:

- Update your invoice payment policies – make it impossible for a single staff member to pay any invoice without making sure it’s valid and make it mandatory for a manager to sign off on all payments.
- As per other crimeware, like cryptolocker, warn staff to beware of any e-mail from an unknown address.
- Engage Evotec to install Sophos Advanced threat protection.

Beware trojans and malware

The CryptoLocker trojan is a good example of the need to train staff in IT security, as well as provide a robust security environment. This particular trojan arrives in your e-mail box as an e-mail pretending to be from a well-known source like Australia Post or Fedex. The e-mail may contain a plausible message about some kind of delivery and what looks like a PDF form.

The PDF turns out to be a zip file carrying a CryptoLocker trojan which encrypts all the files on the user's computer and, if possible, the entire network. The only way to restore these files is to pay a "ransom" for the private key used for the encryption.

Since it's never a good idea to pay a ransom, this can put your network and e-mail out of action for 24 hours while we clean the virus and restore your files from backup.

How to avoid trojans and malware

- Make sure all staff are aware of the dangers of e-mail virus and trojan attack
- Invent in a fully-featured firewall that includes e-mail security
- Only open email attachments that come from a trusted source and that are expected
- Scan email attachments with security software prior to opening – ideally this would happen automatically with a next-gen firewall such as Sophos XG Firewall
- Avoid Spam: Messages that do not include your email address in the TO: or CC: fields are often common forms of Spam
- If you suspect an email is spam, do not respond, just delete it
- Consider disabling the email's preview pane and reading emails in plain text
- Always treat as suspicious requests for confidential information via email. Phishing attacks may use scare tactics or some plausible request to entice a response
- Phishing attacks may consist of a group of emails that share similar properties like details in the header and footer
- Check the authenticity of a suspicious request before responding in email.
- Make sure your backup and restore procedures are working. That means test them!
- Install business-grade Security software to protect all devices, all servers and all applications – including WiFi – on your network from attacks. The costs will be more than outweighed by the time saved in avoiding malware attack. Remember – under the Privacy Act, businesses that keep customer records are required to keep them securely
- Make sure your staff have strong passwords and change them regularly
- Keep security patches up to date

Evotec is a Sophos Gold Partner with a Sophos Architect on staff. We are also a Fortinet Partner – so we can design and implement a total IT security solution for your business.