Some of us received some very enlightening information from Tom Miller yesterday on social engineering. When it comes to ***information security*** the definition of social engineering is - **the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.**

Some surprising examples of this include things you might respond to for fun on a weekly basis such as:

A study performed by **Micke Ahola** of u**secure**, a company in Manchester, United Kingdom [https://www.usecure.io/en/] found that 39% of employees at a company still gave away their passwords in a phishing simulation appearing to come from their own HR department. You will find part of the study and statistics below. The active link above goes to Micke's study **[shared with permission]** and the different types of social engineering we have all been duped into falling for. We are not always the victims of hackers - sometimes we do it to ourselves!

39% of Employees Gave Away Their Passwords In This Phishing Simulation

Micke Ahola

How were employees duped into giving up their passwords?

Most employees sign into apps like 0365 every day - causing them to enter their credentials almost automatically when presented with what looks like a log-in screen.

The employees that followed the link were presented with an Office 365 log-in screen - ostensibly required to verify their identities before allowing them access to the Holiday & Sick Pay policy. The landing page itself is an almost exact replication of a real Office 365 log-in screen - a reasonably easy feat for a cyber criminal to accomplish as it only requires copying the HTML and CSS code from the real log-in page.

The 68% of employees who followed the link the email saw this landing page. 58% of them entered their email address and password.

While the page itself would not give a user any clues about the real owner of the form, the domain name tells a different tale. When entering your credentials online, it's important to always check the domain name of the site. This is because while making your page imitate another page is quite trivial, faking the domain name is a lot harder.

In this case, the domain reads **microloft.com** - not **microsoft.com**, which is the domain where a real Office 365 log-in page would be located. At a quick glance, the domains do look very similar - but this

is not much of a consolation when a cyber criminal has already ran away with your passwords.

What happened afterwards?

The members of staff who clicked the link found out they had been duped.

Instead of finding the juicy details of a new holiday policy, the employees that entered their credentials on the landing page were greeted with a message asking them to contact their IT team. Their passwords were not sent forward to us or anyone else, or recorded in any manner. Had this been a real phishing attack, however, all passwords that had been entered here would now be in the hands of a cyber criminal - with potentially disastrous results.

When a cyber criminal gains a user's email password, a whole world of opportunity opens up for them. Any sensitive or confidential data contained in the user's emails and attachments are now available for the cyber criminal. Since most users use their work email as the back-up or authentication for services like Google Drive, Slack, Hubspot, Trello, Office 365 etc., the attacker would also gain access to these accounts and all data within. A patient attacker, however, would not use this data or make themselves known, but rather stay quiet, monitor email activity to learn more about the business, and wait for the most opportune moment to strike when they can extract the most value out of the business.

If an attacker gained access to not just one email, but the emails of 39% of the company's employees, you can only imagine the type of havoc they could cause.

The full simulation results

The majority of staff opened the email and followed the link - and 39% ended up giving away their passwords.

This phishing simulation had a high 'success' rate - but it's not too dissimilar from the numbers we see from other organisations without existing security awareness training in place.

Here are the full results:

Received	Opened	Visited	Compromised
73	57	50	29
100%	78%	68%	39%

And here's an explanation of what the different categories mean:

Received: How many employees were sent - and successfully received - the email.

Opened: How many employees opened the email by clicking or tapping on it.

Visited: How many employees followed the link in the email.

Compromised: How many employees gave away their log-in details on the phishing page.

How did our client benefit from this?

The good news, as far as our client is concerned, is that they have now fully identified the human threat facing their organisation. Their employees are now all enrolled onto security awareness courses

encompassing not only email and phishing awareness but also topics including safe use of removable devices and the risks of data interception on public Wi-Fi networks.

This simulation allowed our client to:

- **Discover the company's risk level** and vulnerability to human error
- **Raise awareness about security** in a memorable manner among all staff
- **Identify employees in need of extra training** which was automatically provided to them through usecure's automated training

In a couple of months, our client may choose to send out another simulated phishing campaign to see how their employees fare after some training - or they may wish to turn on our auto-phish feature, which constantly selects random employees to test with a templated attack from our library.

What can you do to protect your own organisation?

Regular training and testing is key to protecting your business from phishing scams.

With Accenture recently estimating the total global cost of cyber crime over the next five years to be $5.2 trillion, your business simply can't afford to leave itself unprotected. Security awareness training addresses cyber breaches at the very core - the natural tendency of

untrained users to make mistakes. Simulated phishing works best when used to complement training, as it gives users an opportunity to put what they've learned into practice, as well as letting you assess how effective training has been at improving outcomes.

No technical solution is capable of stopping your employees from making errors, but with the right tools you can turn your end-users from your weakest link into your first line of defense.