DD WEST LLP

"Online Scams and Strong Passwords: Stay alert and cautious"

Author- Orvel L. Currie
Last updated: 04/21/2020

The most common method of attack is the "email spoof". An email is received asking for rapid action or asking you click on something to review it. This form of attack can be concerning as it frequently appears just legitimate enough to deceive the reader into believing they should respond. Typically, the email has elements about it that make the reader somewhat uncomfortable. So, if you receive an email which seems legitimate but leaves you somewhat puzzled or questioning to even the most minor degree, review the email address by putting your mouse cursor over the email address. Particularly scrutinize emails that request you to act quickly or urgently. Look for emails requesting that certain typical transactions processes be altered as to where or how they are to be sent. So be **cautious** with payment of account requests either providing payment or requesting payment. In either case the matter should be referred to accounting department of your organization.

A second method around for over 40+ years is called "social engineering". The concept is that a caller will obtain information from someone in your organization by pretending to be a vendor, client or another member of the firm. A typical example is that reception or an assistant will get a call from a client who wants clearly sensitive information including passwords or personal information about someone. THERE IS NO INSTANCE in which your organization's passwords or personal information should be shared with a client or someone pretending to be a staff member. The cyber criminals are becoming more and more sophisticated. An example would be to receive a call asking to speak to a lawyer/expert. Rather than responding that the lawyer is in Court, respond to the caller that you will leave a message for the lawyer and they will call you when they are available. Additionally, do not leave information on your voice mail or email that you will be away from the office, on holidays or in court. Simply forward your voicemail to an assistant who can assess the legitimacy of the caller. The information on these sources provides information which can be used by the recipient to send to our accounting department, and they respond because it contains an element of truth.

The third method is much more difficult which involves capturing information sent or received from a computer. This is very sophisticated and difficult form of hacking and unlikely unless we are directly targeted. Our system is designed to prevent such attacks. At DD WEST LLP we have specially provided devices to our staff to ensure we have the proper protection. It is important that **YOU DO NOT USE the firm devices for your personal use.** There are several security concerns that personal use puts firm devices at risk. The firm software is not configured to protect against personal use. To a large extend this prohibition is on the "honor system" however if there is evidence of personal use firm on firm devices management must determine an appropriate form of discipline including the loss of the privilege to work from home.

3 more thoughts for your cybersecurity knowledge!

1. Any email you receive that comes from a sender you do not know, is not specifically addressed to you, and promises you benefit is likely to be spam and a scam.

2. A version of the email spoof includes the imbedding of malicious software—also called malware, spyware, key loggers, trojan horses, or trojans. Scammers try to install software on your computer so they can gain access to files stored on your computer and other personal details and passwords. Scammers use a wide range of tricks to get their software onto your computer. They may trick you into clicking on a link or pop-up message in a spam email, or by getting you to visit a fake website set up solely to infect people's computers. (Ransomware) Online auctions and Internet shopping can be a lot of fun and can also help you find good deals. Unfortunately, they also attract scammers. The firm software is not configured to protect against personal use on non-business and potentially risky sites.

3. The computer/email variant of a Phishing scam are all about tricking you into handing over your personal and banking details to scammers. The emails you receive might look and sound legitimate but in reality genuine organizations like a bank or a government authority will never expect you to send your personal information by an email or online. Scammers can easily copy the logo or even the entire website of a genuine organization. So don't just assume an email you receive is legitimate. If the email is asking you to visit a website to "update", "validate" or "confirm" your account information, be sceptical. Phishing emails can carry viruses that can infect your computer. Do not open any attachments or follow any links in phishing emails. Don't reply to spam emails, **even to unsubscribe**, and do not click on any links or call any telephone number in a spam email. Delete it immediately without "clicking" on the contents, then notify IT. Always ask yourself before opening a suspect email, ***will this be worth the risk and will I be risking the security of my computer***?

You need to watch out your “6” when it comes to online scams, and to make that easier you need to have a strong password.
Cryptography is the science of using math to encrypt and decrypt passwords. We all know using 1,2,3,4,5 is a weak password and using your children’s, husbands or dogs name is just as weak. Think social engineering, someone can find that information on Facebook.

So, what makes a strong password? Surprisingly very little effort. To understand how to make a strong password combination you do not have to read **“A course in Number Theory and Cryptography”** by Neal Koblitz or **“Differential Cryptanalysis of Data Encryption Standard”** by Eli Biham et. A well-developed password created using the methods set out here will given today’s computing power and time, (with 1 billion computers doing 1 billion computations per minute) will not decrypt a strong password before the end of the universe.

Well interestingly any 15-character random stream will protect you until the end of the universe! So think of it like this no more complicated #5$&80^ type passwords. If we think about 15-characters you can pick 3-5/6 letter words like **“private selling glasses”.** Any 3 random words will do. If you want to make it to the end of two universes add a character anywhere in the sequence, like a $, #, or &. The magic is not in the words themselves but how random they are with respect to each other. In our example password we have 7+7+6 characters or 20 characters well past the minimum 15 needed for impenetrable security. If the right 3 random words are used, you can memorize the 3 words and the added character and remember your (very strong almost impenetrable) password easily.

Now think why would I say almost impenetrable? We are human so guess what; we are very lazy and at times not bright. We don’t want to create and remember strong passwords! We put our passwords in our phones under notes where they are readily available to anyone accessing your phone. Or better yet we put the password on the bottom of our monitors or carve it into our desks. We use our children’s names and then post it all over the internet. Or even worse we simply leave our computers on when we leave the office so any third party can enjoy your credit card and banking information. Please remember to shut off/lock your computers when you are away from it. Once again it is human vulnerabilities that beat cryptography, mathematics and a computer security system.

So please go get your 3 random words – 15 characters’ minimum (you can remember easily) and set up your new passwords. Please do not go on the internet to test your password. We have no idea which programs are legit and which are just listing possible passwords for a brute force attack! You can use these sites to have fun to see how long it will take to crack a password like yours.