CHRISTINA ARCANE *InspireCyber*
info@inspirecyber.com https://inspirecyber.com/
https://www.linkedin.com/in/christinaarcane/

Christina Arcane is the Director and Cyber Security Specialist at InspireCyber, a firm dedicated to engaging non-cyber professionals in the fundamentals of security to protect their business, their assets, their people and their community. Christina has a long spanning career in privacy and security which includes significant roles in the security teams at large organisations, consulting contracts and she was co-founder and operations director of a UK cybersecurity start-up BreachAware (acquired in 2020).

TIP 1. SAVE YOUR FILES IN THE CLOUD

If your computers get hacked, this will protect your information from being stolen or deleted because the attacker needs additional authorisation to locate and access your files. Any files saved in your downloads, or on your desktop, are easily accessible - otherwise and could expose your business.

TIP 2. WHAT IS YOUR EMAIL FORMAT?

Avoid using firstname.lastname@company.com or firstname@company.com email formats. Hackers guess these very easily and you are more likely to receive scam, spam and phishing emails that can do damage to your company. Reduce the noise in your inbox and use an email format that is not easily guessable. For example: elon.mu1@company.com ('Elon Musk' - only the first two letters of your last name and a number).

TIP 3. NEVER OPEN A LINK IN AN SMS NEVER. DON'T DO IT. I'M SERIOUS.

SMS is notoriously unsafe because phone numbers can be ported and spoofed. This means they can't be verified and anyone can impersonate them. Links in messages are also shortened so you can't reveal the real website hiding behind them without clicking on them - and by then it's too late. When you receive an SMS with a link, if you believe it is legitimate, visit the sender's website directly to confirm the information.

TIP 4. CHECK THE SENDER'S EMAIL ADDRESS BEFORE CLICKING

Most phishing emails can be identified as malicious by simply revealing the true email address of the sender in an email but many of us don't stop to take a quick look. This could be because it's not a habit or there is an extra step like clicking an arrow to see the full address. Either way it's an important step to take to prevent a mishap.

TIP 5. DON'T BE BLINDED BY LARGE, QUICK PAYING ORDERS

A nice big order always makes up happy and excited for this new success and sometimes this means we are blinded to the warning signs that it could be a scam, this is the scammers intention. Unfortunately, large orders are the first red flag to scam with payment method, communication, and urgency being the other red flags. Use your due diligence on large orders to avoid sending your product or providing your services and never actually receiving payment.

TIP 6. BE CAREFUL WHICH SITES YOU VISIT TO DOWNLOAD SOFTWARE

There are lots of fake websites out there pretending to be the software you want to use in your business. They can look identical to the real website because hackers can be great graphic designers. The best way to spot this is to look at the web address or URL at the top of the page as hackers can't use the real website address. You can do another Google search to quickly know you're on the right, legitimate website.

TIP 7. LET YOUR CUSTOMERS KNOW ABOUT SOCIAL MEDIA CLONING

Protecting your business is important and your customers are your business. You can't control or stop a malicious actor

from cloning your branding on social media. They may create an identical account and try to contact your customers to scam them. Whilst this isn't your fault, it's your brand and your customers won't be happy with you. When you identify your brand being cloned, let your customers know it isn't you and give them information on the ways you do business so they know not to be tricked by the malicious actor.

TIP 8. DON'T CONNECT ALL YOUR ACCOUNTS

Some websites allow you to login through Gmail. Facebook, LinkedIn or another avenue. This isn't necessarily insecure but I like to follow the rule of thumb in security - keep everything separate. This gives you greater control of your accounts, enabling separate passwords, 2FA and other secure measures so if one of them is compromised, it is not possible to find a way through to the others. It does mean a few extra steps to manage your accounts - for me, it is worth it.

TIP 9. TEACH YOUR PEOPLE THE BASICS OF TECHNOLOGY

Do all your people know how to properly use email, SMS and your digital tools? Often it is a company's people who aren't sure how to use the technology in the business which leads to accidental data leaks, clicking on a phishing email, purchase of fake gift cards or saving a document to the wrong location - and these all lead to disaster for your company. Teaching and helping your team is key to maintaining a strong secure posture as hackers like hacking humans more than computers because after all - we are only human!

TIP 10. HAVE A HACKING PLAN

Take half an hour to research and build a plan on what you would do if your company is compromised by a hacker. What if your information is leaked? What if your customer database is leaked or lost? Who would you call? What is your first step? Do you keep all your computers on? Knowing and having it written down can make all the difference and it won't take much of your time.