NSDA
Nova Scotia Dental Association

T 902.420.0088 **E** nsda@eastlink.ca
F 902.423.6537 **W** www.nsdental.org

Dental Office Cyber Security Basics

(October 2019)

Emails

- If your email is hacked change your password immediately.
- Hide your email address as much as possible – use forms on websites, not email links.
- Don't click on anything – always delete if suspicious.

Train your staff

This does not have to be complicated:

- Discuss with your team – add it to meeting agendas.
- Learn about Ransomware and what to do if it happens to you
- Get feedback from staff on what they are seeing in emails.
- What is the latest scam?
- Lock computer screens when unattended.
- Report anything suspicious
- Provide onboarding and exiting policies for new staff and staff that have left
- Have social media policies in place – have one person only allowed to post
- Don't install any software unless authorized

Passwords

- Keep different ones; don't use the same for all
- Use a password vault such as Keeper or LastPass

Backups

- Full backups and test them to make sure they are working
- Encrypt external hard drives if taking them offsite
- Backup to the cloud as well as external devices

Mobile phone security

- Avoid public Wi-Fi spots
- Use HTTPS websites
- Don't download Apps
- Disable Geotagging Feature
- Get permission before taking any photos
- Report Lost / Stolen device immediately (remote wipe could be initiated)
- Secure all other wireless communications used by your device, such as infrared & Bluetooth
- Never use 'remember me' for passwords

NSDA
Nova Scotia Dental Association

T 902.420.0088 E nsda@eastlink.ca
F 902.423.6537 W www.nsdental.org

Dental Office Cyber Security Basics

(October 2019)

Ransomware

- Do not pay as it is very rare that your data will be unlocked
- Lock down your network quickly so to limit the spread
- Search for free software that can unlock your data
- Email is the main infection method so train your staff to be vigilant
- Backup and test that you can restore from the backup
- Keep software updated

Routine Maintenance

- Run Antivirus software regularly and keep it updated
- Have computer maintenance in place: Windows updates, Router updates, etc
- Make sure your Wi-Fi is secure. Set up a specific ‘guest Wi-Fi’ on your router.
- Keep website hosting up to date
- Keep an IT inventory list so you know what to replace if needed
- Provide a simple cyber risk assessment – keeping credit card details is a higher risk for example.

Other

- Look into the possibility of Cyber insurance, but be careful as it can be very expensive and complicated on what is actually covered. Taking data offsite can void the insurance for example.

- Make sure you are PCI compliant with any credit card details kept in the office. You are not compliant if you are just keeping records in an excel spreadsheet.

- Report a data breech – you have a legal requirement to do so. If a breach creates a “real risk of significant harm” to the affected individuals, then you must report the breach.