THE NAVIGATOR COMPASS NETWORK GROUP

October 2016

In This Issue:

Your PC Recycling Bin Could Cause You MAJOR Problems

Although a lot of stress has been put on policies around network access and data storage security to stop data breaches, one of the biggest sources of cyber breaches are actually – the PC Recycle Bins.

Studies have found that a majority of global IT professionals think that erasing data is the same as deleting data. A study by Blancco Technology Group found that about a third of the IT professionals stated they drag individual files to the Recycle Bin.

There has been a lot of work done with businesses in the finance, healthcare and government sectors to emphasize the necessity of permanently erasing data from IT equipment and devices.

The challenge is that many workplaces underestimate the need to erase active files from computers, laptops, external drives and servers. This means exposing huge volumes of sensitive, confidential and potentially compromising data, making it vulnerable to breaches.

There's obviously a lack of clarity among the majority of users as to how computers actually work when it comes to data removal and data protection.

With the enormous amounts of data being created every day, it's critical that data is safely erased when there's no longer need for it or when required to be removed.

Another issue is storage and handling of IT equipment. Many professionals store non-functional desktop/ laptop computers, external drives and servers in easily accessible, unsecured locations.

The overall need seems to lie in the fact that data retention policies need better implementation, starting with making sure there are written data retention or removal policies.

Contact Compass Today for Assistance: (866) 336-8727

5 Ways to Keep Your Users Safe from Spear Phishing

Spear phishing is a technique used by cybercriminals in which an email that appears to be from a friend or colleague is sent that either encourages recipients to download malicious attachments, click on malicious links, or send sensitive personal or professional information back to the sender.

Unfortunately, once someone takes the bait and clicks on a link in the phishing email their computer can quickly become infected with malware that can steal the user's critical information, wreck their system, or encrypt their hard drive until your company pays an outrageous ransom to the people holding the data hostage.

Here are 5 Tips for Keeping Users Informed and Vigilant About Spear Phishing:

1. Check Twice, Click Once

Before clicking on any links in an email, users should stop and hover over the hyperlink to see the destination URL first, since spear phishers will often hide their URLs in email text with things like "just click here to confirm" or "we just need some more information, please fill out this form", etc.

If the URL that the link is pointing to is not familiar, users should not click on it.

2. If Unsure About Email, Check with the Sender

A favorite tactic of spear phishers is to impersonate executives of a company and send emails to their employees in order to get them to reveal sensitive information.

Users should always check with the sender to confirm the email is legit any time they receive one with a request that seems out of the ordinary, no matter who it says sent it. If that person says they didn't send such email, the matter should be reported to IT immediately.

3. Never Send Confidential Info Via Email

Spear phishers commonly email employees and ask for confidential and sensitive information.

Sending user passwords, W-2s, corporate banking information, or other sensitive info over email is never a good idea. If anyone makes these types of requests, it can be an indication that your company is the target of phishing attacks.

4. Do Not Post Too Much Personal Info Online

Posting too much personal information publicly can help spear phishers successfully breach users' company.

Users should be especially careful not to post their work phone numbers online, as many spear phishers will try calling and pretending to be IT staff or admins to assure users that they should send them the information they requested.

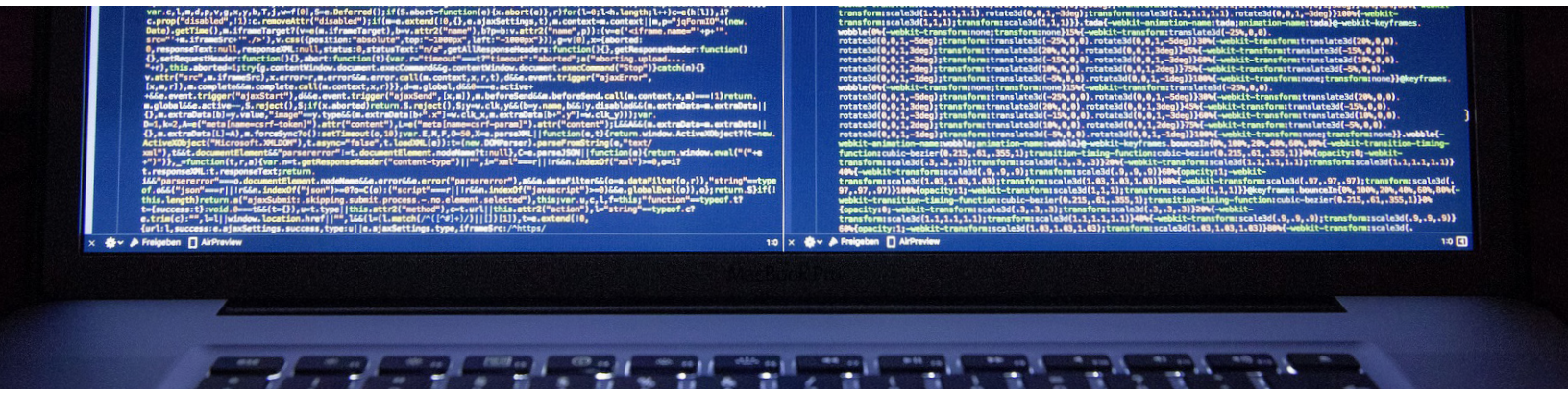
5. Use a Behavioral-Based Endpoint Protection

The fact is that no online strategy, tool, or behavior is going to be effective 100% of the time - sooner or later, someone will click on something that will open a company up to a breach.

This is why a behavioral-based endpoint protection tool will help ensure that, if something suspicious or malicious gets through, the malware infection can be caught and stopped before it does any damage.

Since the potential profits from spear phishing can be great, cybercriminals can be expected to not only continue with it, but also find new ways to attack. **With the right tools, training, and strategy, we can keep users and their company safe.**

CLICK HERE TO READ MORE



 | www.CompassNetworkGroup.com | 866.336.8727

How Hackers Are Taking Advantage of **Windows Troubleshooting Platform**

We are seeing new hacking threats every day, and cybercriminals are now utilizing troubleshooting service to scam users into downloading malware.

Specifically, **Windows Troubleshooting Platform (WTP), a legitimate feature in Windows,** is used to con victims into downloading malware onto their computers.

Luckily, it was discovered by researchers at Proofpoint that a social engineering attack is taking advantage of this service and uses it as a pathway for infection.

The researchers shared that what makes this attack especially successful is that implementation of troubleshooting does not come with a security warning, plus users are used to running it as it appears in Windows.

This malware means that when you run the troubleshooter – you're allowing the installation of LatentBot. It is a well-documented modular bot used for surveillance, information stealing, and remote access.

This is what the scam looks like:

The targeted user will receive an email with a file attachment; when downloaded and opened, an issue with the computer's font set will appear, and he or she will be prompted to "double-click to auto detect charset". This will lead to a real embedded, digitally signed DIAGCAB file, the extension for a Troubleshooting pack. Once opened, it will display a window that Proofpoint calls a "convincingly realistic" download wizard. If the user clicks "next", it will download and execute the malware payload on the computer.

The researchers explain that this malware bypasses detection of many existing sandbox products, due to **the malicious activity being carried out outside of the msdt.exe binary loading the .diagcab file.**

Finding ways to evade sandbox via COM-based non-standard execution flow is a new trend in cybercrime. This malware method can trick even the experienced users, since it's very convincing and bypasses detection of many sandboxing techniques.

Dedicated Compass team can help your practice be **compliant and your patient information secure - seek Compass Network Group expert IT solutions.**

Navigate to better dentistry-specific technology today: (866) 336-8727.

