



POWERED BY  DUG

DYNAMICS CON LIVE

MAY 2024

Hackers and Phishers and Link Clickers, Oh My!



Mike McPhilomy

Director of Sales and Marketing

14 years in the GP Community
Passionate about helping GP Customers and
Partners develop and implement their Cloud
Strategy



Session Agenda

- Password Hygiene
- Protecting your Wi-Fi Hotspots
- Staying Safe on Public Wi-Fi and charging stations
- How to Identify Phishing Emails
- Protecting your devices and backups





Password Hygiene

The Evolution of Passwords

dakota



The Evolution of Passwords

Dakota



The Evolution of Passwords

Dakota1



The Evolution of Passwords

Dakota1!



The Evolution of Passwords

Dakota2!



The Evolution of Passwords

Dakota43!



The Evolution of Passwords

d@k0tA43





Key	
m – Million	tn – Trillion
bn – Billion	qt - Qintillion



Password Best Practices

- Use Multi-Factor Authentication
- Only change passwords when there is a breach
- Don't write your Passwords down
- No need for complex passwords
- Simple, Long and Memorable
- CorrectHorseBatteryStaple is better than d@k0tA43
- Use a different password for every app/site



Password Manager

- Runs on all your Devices
- Will identify re-used passwords
- Generates random 16-24 character passwords
- You only have to remember 1 pass phrase





Protecting Your Wi-Fi Hotspots

Protecting Your WiFi Hotspots

- Don't use the default Admin Password
- Don't use the default Network Name
- Use 16–24 Character Pass Phrases
- Keep the Router Firmware Updated



Protecting Your WiFi Hotspots

- Turn Off
 - Plug 'n Play (UPnP)
 - Remote Management
 - WiFi Protected Security (WPS)
- Turn On
 - Router Firewall
- Consider a separate WiFi Router for Work Devices



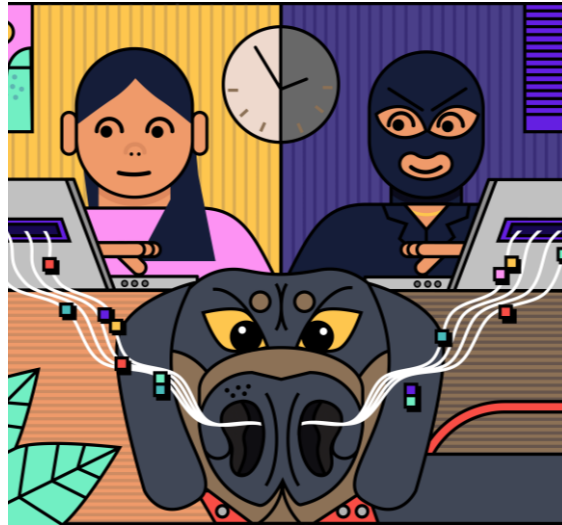


Staying Safe on Public Wi-Fi and Charging Stations

Know Your Risks



Evil Twin



Packet Sniffer



Juice Jacking



Keeping Safe in Public

Public WiFi

- Connect to your Office VPN
- Purchase VPN Software

Public Charging Stations

- Bring your own cables
- Plug into an Wall Outlet, not a USB port





How to Identify Phishing Attacks

Two Types of Phishing Attacks

Phishing

- Cast a Wide Net
- Email that appears to be from someone you know or a company you trust
- Request to click on a link or open a ZIP file that downloads malware to your device

Spear Phishing

- Targeted
- Customer/Employee request to change bank accounts
- Owner/Boss asks accounting to send a wire



How to Identify a Phishing Attack

Use Critical Thinking

- Does this person normally send me OneDrive Links, Project Updates or Invoices?
- How are changes to bank accounts and payment methods normally handled?
- Pay attention to your Spidey-Sense



How to Identify a Phishing Attack

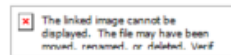
Look Closer

- Look at the actual email address of the sender (not the display name)
- Hover over the 'Click Here' phrase and the actual URL will be displayed in a pop-up menu



Your Password is About to Expire

The screenshot shows an Outlook email window. At the top, the header includes 'FROM: Office 365 Team', 'SUBJECT: Your password is set to expire', 'RECEIVED: Thu 3/8/2018 ...', 'SIZE: 61 KB', and 'CATEGORIES'. The email body contains the following text: 'Dear Cdobkins We detected your password is due to expire in 24 hours. Extend your password expiry time to a later date to avoid being disconnected from our services'. Below the email content is a ribbon with tabs for 'File', 'Message', and 'Help'. The 'Message' tab is active, showing various actions like 'Ignore', 'Delete', 'Archive', 'Reply', 'Reply All', 'Forward', 'Move to Archive', 'Deleted Items', 'Accounting', 'To Manager', 'Move', 'Assign Policy', 'Mark Unread', 'Categorize', 'Translate', and 'Editing'. The email header shows the sender as 'Office 365 Team' with a contact ID and email address, and the recipient as 'Chris Dobkins'.



Dear Cdobkins

We detected your password is due to expire in 24 hours.

Extend your password expiry time to a later date to avoid being disconnected from our services

Kindly extend your password immediately by visiting our web link below:

Where this link REALLY goes:
<http://teejaykahlani.de/gates/index.php?94a08da1fecbb6e8b46990538c7b50b2=c4ca4238a0b923820dcc509a6f75849b&373fb707008072792e09a4d6d2def998=3f01be9501c5365303e4aaf2b8cea40b&id=1&email=cdobkins@njevity.com>

<https://microsoftonline.com/expiry/renew/password>



Some of your Messages were not Sent

Microsoft Message Delivery <deliveryfailure@computer.email.mil>
Some of your messages were not sent Successfully

To: Chris Dobkins

If there are problems with how this message is displayed, click here to view it in a web browser.

Where this link REALLY goes:

<http://zanestop10.com/.b/?th=cdobkins@njevity.com>

Your Messages Has Not Been Sent

Hi cdobkins@njevity.com

We recently encountered an outgoing server failure which left Most of your mails undelivered. Some of your mails were affected and can be resent now.

[Click here](#) to resend these mails.

Microsoft and Office365 team are always working to give you the best email experience. We are sorry for any inconvenience caused.



Report Phishing Attacks

Anti-Phishing Working Group (APWG):

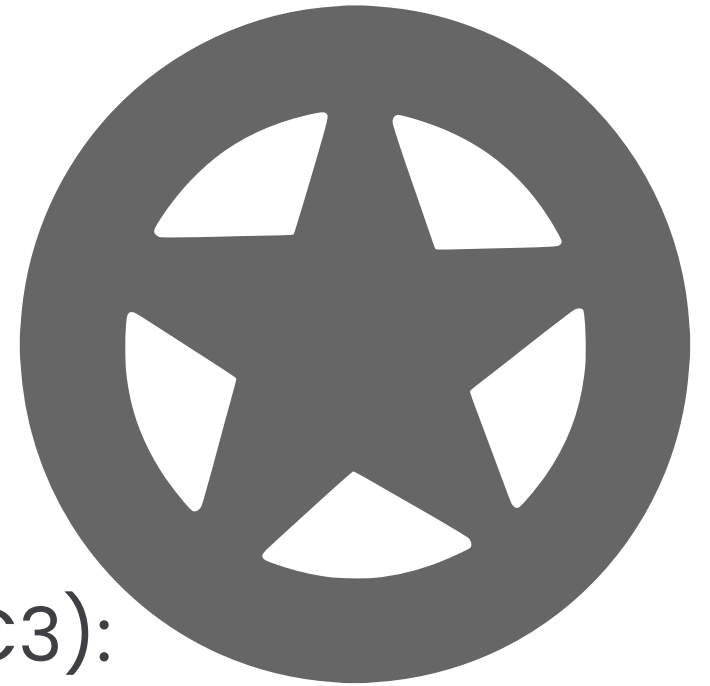
<https://antiphishing.org/report-phishing>

Federal Trade Commission:

<https://reportfraud.ftc.gov>

FBI's Internet Crime Complaint Center (IC3):

<https://www.ic3.gov>





Protecting Your Devices

Keep your Devices Safe*

Windows

- Apply Updates
- Anti-Malware

MacOS

- Apply Updates
- Anti-Malware

Android

- Apply Updates
- Anti-Malware

iPhone

- Apply Updates

***Don't let your kids use your work devices**



Keep Your Backups Safe

- The bad guys are looking for your backups
- Find an Online Backup Service that is built with Ransomware in mind.
- Periodically backup to a removable disk... and then remove it




Now What?



- Buy a Password Manager
- Change all of your passwords for every online site/app you use
- Change the passwords on your WiFi Router
- Use a VPN on Public WiFi
- Keep your Devices up-to-date (including your WiFi Router)
- Don't use public charging stations





Q&A