Protecting Senior Citizens from computer crimes.

Presented to the Kiwanis club of Albany on 8-15-24

by Nate Tuenge – Nerd & computer guy

Why should we listen to Nate?

- Owned and built computers since I was in middle school.
- I have worked in cybersecurity sales for 5+ years for companies like Symantec & Bitdefender.
- Attended Lane Community College and attained an Associates in Computer Network Operations.
- Became CompTIA – Network+ certified.

This means I passed standardized testing on how computers talk to each other and network security principles.

Common types of cyber crime

Malware – malicious software that can harm a computer system or user.

- **Viruses & Worms –** software that corrupts the system or destroys data.
- **Spyware & Adware –** software that might look legitimate but has other nefarious purposes. (EX. A solitaire program that is also a key logger that can steal passwords)
- **Ransomware –** software that uses encryption to hold the computer or files hostage until a fee can be paid.

Common types of Cyber Crime – cont.

Social Engineering – using deception to manipulate individuals into providing personal or confidential information for fraudulent purposes.

- **Phishing / Smishing –** fraudulent emails or text messages that spread malware or trick people into giving sensitive information through fake websites. (credit cards, SSN #, passwords)
- **Baiting -** social engineering attack that lures victims into providing sensitive information or credentials by promising something of value. (lottery scams or “free” music / movie to downloads)
- **Pretexting -** form of social engineering where attackers focus on creating a pretext, or a fabricated scenario, that they can use to steal someone's
- **Scareware -** social engineering in which a scammer inserts malicious code into a webpage that causes pop-up windows with flashing colors and

Social Engineering Process

Preparing the ground for the attack:

- Identifying the victim(s).
- Gathering background information.
- Selecting attack method(s).

Deceiving the victim(s) to gain a foothold:

- Engaging the target.
- Spinning a story.
- Taking control of the interaction.

Obtaining the information over a period of time:

- Expanding foothold.
- Executing the attack.
- Disrupting business or/and siphoning data.

Closing the interaction,
ideally without arousing suspicion:

- Removing all traces of malware.
- Covering tracks.
- Bringing the charade to a natural end.

Smishing example

Things to watch out for:

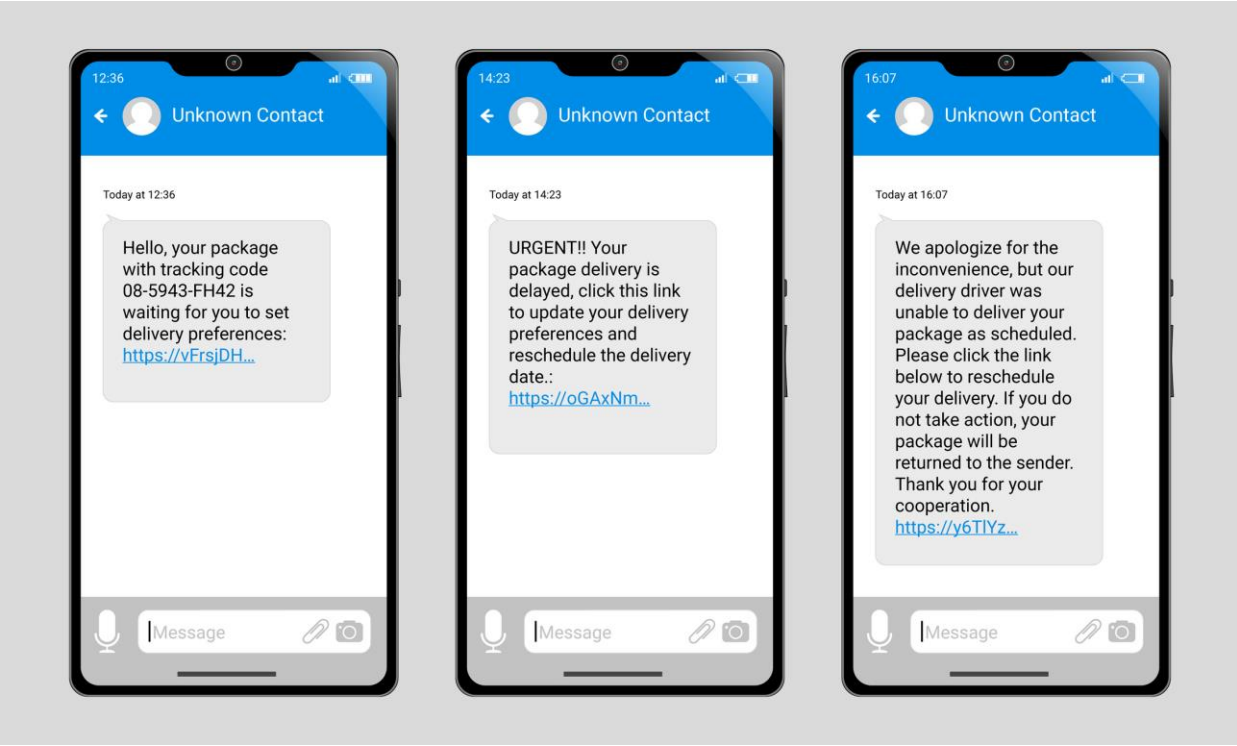
Unknown number / phone number / sender who is not in your address book

Parcel Tracking is something you have to signup for. (not typically automatic)

Website link doesn't start with www or look official. (don't click!)

False sense of urgency.

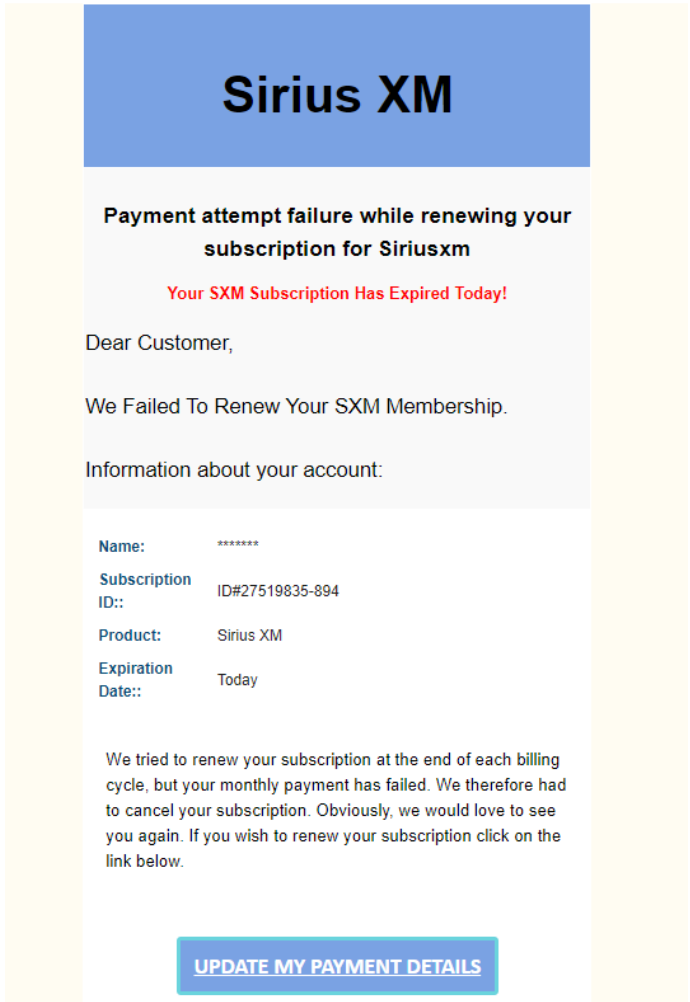
Spelling or grammar issues.



Common themes in phishing

- **Suspicious sender's address.** The sender's address may imitate a legitimate business. Cybercriminals often use an email address that closely resembles one from a reputable company by altering or omitting a few characters.
- **Generic greetings and signature.** Both a generic greeting—such as "Dear Valued Customer" or "Sir/Ma'am"—and a lack of contact information in the signature block are strong indicators of a phishing email. A trusted organization will normally address you by name and provide their contact information.
- **Spoofed hyperlinks and websites.** If you hover your cursor over any links in the body of the email, and the links do not match the text that appears when hovering over them, the link may be spoofed. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net). Additionally, cybercriminals may use a URL shortening service to hide the true destination of the link.
- **Spelling and layout.** Poor grammar and sentence structure, misspellings, and inconsistent formatting are other indicators of a possible phishing attempt. Reputable institutions have dedicated personnel that produce, verify, and proofread customer correspondence.
- **Suspicious attachments.** An unsolicited email requesting a user download and open an attachment is a common delivery mechanism for malware. A cybercriminal may use a false sense of urgency or importance to help persuade a user to download or open an attachment without examining it first.

Phishing example



Sirius XM

Payment attempt failure while renewing your subscription for Siriusxm

Your SXM Subscription Has Expired Today!

Dear Customer,

We Failed To Renew Your SXM Membership.

Information about your account:

Name:	*******
Subscription ID::	ID#27519835-894
Product:	Sirius XM
Expiration Date::	Today

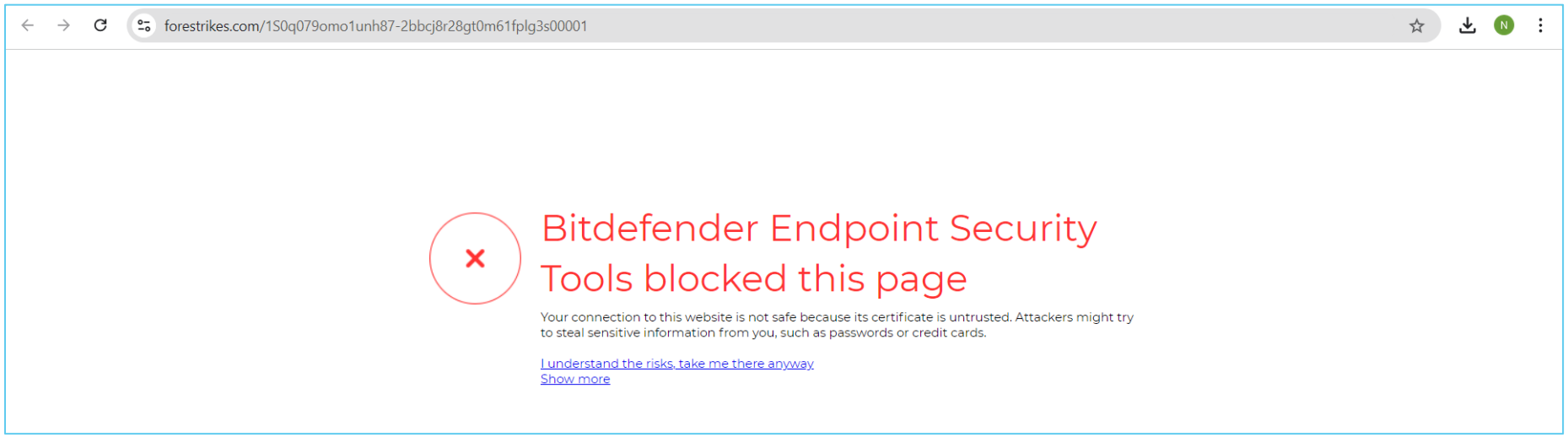
We tried to renew your subscription at the end of each billing cycle, but your monthly payment has failed. We therefore had to cancel your subscription. Obviously, we would love to see you again. If you wish to renew your subscription click on the link below.

UPDATE MY PAYMENT DETAILS

“Fishy” things to look for?

- Unknown sender
- Services you don’t have/use
- Website link doesn’t start with www. or https:// or look official. (don’t click!)
- False sense of urgency.
- Spelling or grammar issues.
- Did not specifically reference me (dear “Customer).

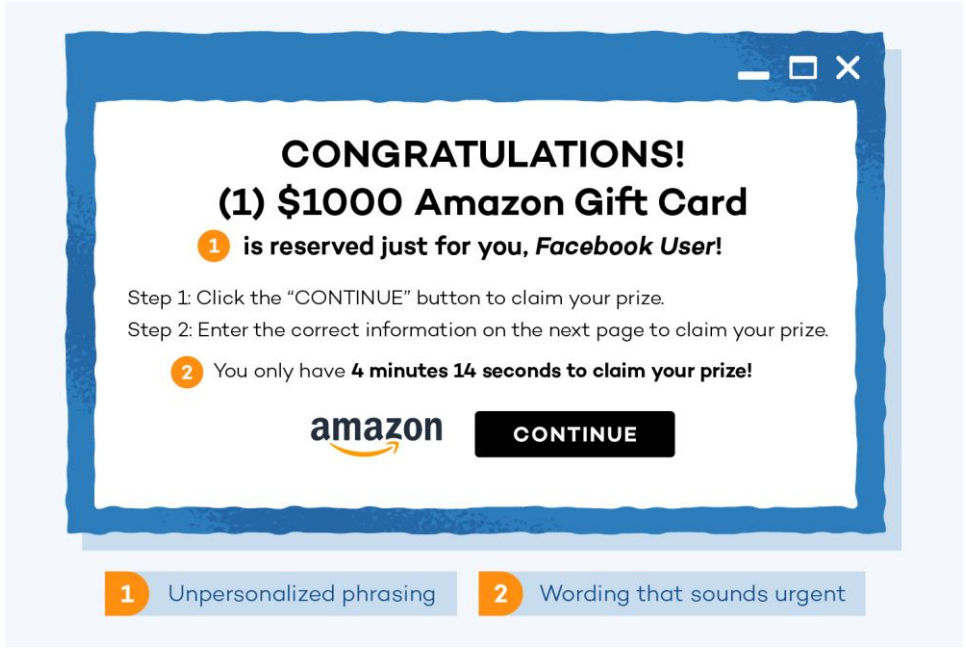
Phishing example cont.



Website lookup tool > ICANN = Internet Corporation for Assigned Names and Numbers, is a nonprofit organization that manages the internet's unique identifiers.

i.e. how the space on the world wide web such as www.microsoft.com is register to one owner; in this case the Microsoft Corporation. This help prevents other companies from having the same website on the world wide web.

Baiting example



Pre-texting example

!! URGENT !! - employee code of conduct update Inbox ×

SUPPORT <support@notyourcompany.com>
to me

Dear [Employee],

Please e-sign your name on the last page of this document to acknowledge that you have read and understood the changes in the employee code of conduct agreement.

Employee code of conduct agreement

You must sign for the changes **within 48 hours** of receipt of this email, or probationary action may be taken.

Kind regards,

Management Team

Scareware examples

Top Scams according to AARP

6 Top Scams to watch out for in 2024

- Check cooking scam
- Voiceprint scam
- Delayed-action sweepstakes scam
- Virtual celebrity scam
- Multistage Grandparent scam
- Paris Olympic scam

How to protect yourself

- Delete emails & SMS from unknow senders (don't REPLY! that lets them know you exist.)
- Use an antivirus on computers, mobile devices, and cellphones. There are free versions from trusted security vendors but I would recommend a paid subscription for more advanced security and protection.
  - PC magazine article – paid versions.
  - Free computer versions:
    - AVAST
    - AVG
    - Malwarebytes
    - Windows Defender (should be pre-installed on most windows systems)
- Don't pickup phone calls from unknown numbers.
- TRUST YOUR GUT! – is this thing too good to be true?
- Look up numbers from official sources do not trust the numbers in emails/text messages.
- Visit the Cybersecurity & Infrastructure Security Agency (CISA) website to learn more.

Thank you!